

1 FAM 260

BUREAU OF DIPLOMATIC SECURITY (DS)

(CT:ORG-344; 08-29-2014)
(Office of Origin: DS/MGT/PPD)

1 FAM 261 ASSISTANT SECRETARY FOR DIPLOMATIC SECURITY (DS)

1 FAM 261.1 Responsibilities

(CT:ORG-344; 08-29-2014)

- a. The Assistant Secretary for Diplomatic Security (DS) reports directly to the Under Secretary for Management (M);
- b. The Assistant Secretary reports to the Secretary as threats and circumstances require, and carries out, by delegation of authority, DA-214, the Secretary's security responsibilities under the Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended (22 U.S.C. 4802 et seq.), for:
 - (1) Serving as the primary advisor to the Secretary, Deputy Secretaries, Under Secretaries and Assistant Secretaries of State on all security and law enforcement-related matters at all DOS facilities abroad and within the United States.
 - (2) Establishing and operating post security and protective functions abroad;
 - (3) Developing and implementing communications, computer, and information security;
 - (4) Emergency planning abroad;
 - (5) Establishing and operating local guard services abroad;
 - (6) Supervising the U.S. Marine Corps security guard program;
 - (7) Liaising with U.S. private-sector security interests abroad;
 - (8) Protecting foreign missions and international organizations, foreign officials, and diplomatic personnel in the United States, as authorized by law;
 - (9) Protecting the Secretary of State and other persons designated by the Secretary of State, as authorized by law;
 - (10) Physically protecting Department facilities, communications, and computer and information systems in the United States;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (11) Conducting investigations relating to protection of foreign officials, diplomatic personnel, and foreign missions in the United States; suitability for employment; employee security; illegal passport and visa issuance or use; and other investigations; as authorized by law;
 - (12) Carrying out the rewards program for information concerning international terrorism authorized by 22 U.S.C. 2708;
 - (13) Performing other security, investigative, and protective matters as authorized by law;
 - (14) Developing and coordinating counterterrorism planning, emergency action planning abroad, threat analysis programs, and liaison with other Federal agencies to carry out these functions;
 - (15) Developing and implementing technical and physical security programs, including security-related construction, radio, and personnel security communications, armored vehicles, computer and communications security, and research programs necessary to develop such measures;
 - (16) Managing the Diplomatic Courier Service;
 - (17) Developing facilities, methods, and materials to upgrade necessary skills to carry out these responsibilities; and
 - (18) Managing and developing antiterrorism assistance programs to assist foreign government security training that are administered by the Department under chapter 8 of part II of the Foreign Assistance Act of 1961 (22 U.S.C. 2349aa et seq.).
- c. The Assistant Secretary assists the Secretary of State and the Under Secretary for Management with formulating policy on security programs worldwide for the Department and the foreign affairs community serving abroad under the authority of the chiefs of missions;
 - d. The Assistant Secretary chairs the Overseas Security Policy Board (OSPB), whose members include the security directors of the foreign affairs and intelligence agencies represented at U.S. diplomatic and consular missions abroad;
 - e. The Assistant Secretary advises the Secretary and the Under Secretary for Management on diplomatic security matters and supervises the Bureau of Diplomatic Security;
 - f. The Assistant Secretary coordinates the provision of diplomatic security services and the exchange of security-related intelligence and operational information among the Department, foreign governments, other U.S. Government agencies, and all law-enforcement authorities; and
 - g. The Assistant Secretary has overall substantive and coordinating responsibility for the following Department regulatory publications:
 - (1) 1 FAM 260, Bureau of Diplomatic Security (DS); and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (2) Foreign Affairs Manual (FAM), Volume 12 —Diplomatic Security and its related Foreign Affairs Handbooks (FAHs) in their entirety including:
 - (a) 12 FAH-1, Emergency Planning Handbook;
 - (b) 12 FAH-2, Protection Handbook;
 - (c) 12 FAH-3, Field Office Management Handbook;
 - (d) 12 FAH-4, Investigations Handbook;
 - (e) 12 FAH-5, Physical Security Handbook;
 - (f) 12 FAH-6, Overseas Security Policy Board (OSPB) Security Standards and Policy Handbook
 - (g) 12 FAH-7, Local Guard Program Handbook (LGP);
 - (h) 12 FAH-8, Residential Security Program Handbook;
 - (i) 12 FAH-9, Special Protective Equipment Handbook;
 - (j) 12 FAH-10, Information System Security Controls and Procedures; and
 - (k) 12 FAH-11, Technical Security Handbook.
- h. Managing the Directorate of the Executive Director for Diplomatic Security (DS/EX):
 - (a) Deputy Executive Director;
 - (b) Office of Management Services (DS/EX/MGT);
 - (c) Office of the Chief Financial Officer (DS/EX/CFO);
 - (d) Office of the Chief Technology Officer (DS/EX/CTO); and
 - (e) Human Resources Management (DS/EX/HRM).

1 FAM 261.2 Organization

(CT:ORG-344; 08-29-2014)

See 1 FAM Exhibit 261.2 for the Bureau of Diplomatic Security organization chart..

1 FAM 261.3 Authorities

(CT:ORG-290; 10-31-2012)

- a. DS was established within the Department pursuant to the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Public Law 99-399; 22 U.S.C. 4801, et seq.). Title I of the Act defines the security functions and responsibilities of the Secretary of State. Title II of the Act authorized the creation of the Diplomatic Security Service, which is responsible for managing the Bureau of Diplomatic Security's day-to-day security operations. Title III of the Act provides that the Secretary of State must convene accountability review boards. The Secretary delegates responsibility to the Assistant Secretary for Diplomatic Security for

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

those functions vested in the Secretary of State by sections 103(a)(2) (22 U.S.C. 4802(a)(2)) and 402(a)(2) (22 U.S.C. 4852(a)(2)) of the Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended by section 162(g) of the Authorization Act; and the functions vested in the Secretary of State by section 214 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 4314);

- b. Section 103(a)(2) (22 U.S.C. 4802(a)(2)) provides for the following security functions: The Secretary of State must develop and implement (in consultation with the heads of other Federal agencies having personnel or missions abroad where appropriate and within the scope of the resources made available) policies and programs, including funding levels and standards, to provide for the security of U.S. Government operations of a diplomatic nature and foreign government operations of a diplomatic nature in the United States. Such policies and programs must include:
 - (1) Protecting all U.S. Government personnel on official duty abroad (other than Voice of America correspondents on official assignment and those personnel under the command of a United States area military commander) and their accompanying dependents;
 - (2) Establishing and operating security functions at all U.S. Government missions abroad (other than facilities or installations subject to the control of a U.S.-area military commander);
 - (3) Establishing and operating security functions at all Department facilities in the United States; and
 - (4) Protection of foreign missions, international organizations, and foreign officials and other foreign persons in the United States, as authorized by law.
- c. The Overseas Security Advisory Council (OSAC) was established pursuant to the Federal Advisory Committee Act (Public Law 92-463) 5 U.S.C. App. 2, section 1 et seq. (See also 12 FAM 024.);
- d. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 and National Security Policy Directive 1 (NSPD-1) provide authority for the Overseas Security Policy Board (OSPB);
- e. The legal authorities for the Freedom of Information and Privacy Act Program within DS (12 FAM) are:
 - (1) 22 CFR 171, Availability of Information and Records to the Public;
 - (2) 5 FAM 414.4 and 5 FAM 414.6;
 - (3) The Freedom of Information Act (FOIA) 5 U.S.C. 552 (Public Law 89-487), as amended;
 - (4) The Privacy Act of 1974, 5 U.S.C. 552a (Public Law 93-579), as amended; and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (5) Executive Order (E.O.) 13526 (classified national security information).
- f. Section 36 of the State Department Basic Authorities Act of 1956 (Public Law 84-885), as amended (22 U.S.C. 2708), provides authority for the counterterrorism rewards program;
 - g. Section 37 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2709) provides authority for certain responsibilities of Diplomatic Security special agents (i.e., passport and visa fraud, investigations, protection);
 - h. Section 160 of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (Public Law 100-204), as amended, provides authority for construction security certifications;
 - i. Section 103 (a)(2)(G) of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 and Part II of the Foreign Assistance Act of 1961 (Public Law 87-195), as amended (22 U.S.C. 2349aa), provide authority for the antiterrorism assistance program;
 - j. Under the Foreign Missions Act of 1982 (as codified at 22 U.S.C. 4314), and 18 U.S.C. 3056A(d), the Department provides for the extraordinary protection of foreign missions and officials, international organizations and foreign dignitaries under certain circumstances throughout the United States. (See also Executive Order 12478 (1984) and Delegation of Authority No. 214, Section 8 (1994).);
 - k. The Bureau of Diplomatic Security has authority to conduct personnel security and suitability investigations based on the following executive orders and laws:
 - (1) Section 103 (a)(2)(B), Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. 4802(a)(2)(B));
 - (2) E.O. 10450 dated April 27, 1953; and
 - (3) E.O. 12968 dated August 2, 1995.
 - l. Public Law 89-554 (5 U.S.C. 7531 – 5 U.S.C. 7533), enacted September 6, 1966, gives to the heads of major U.S. Government agencies, including the Secretary of State, the power to summarily suspend and remove any employee of the agency when deemed necessary “in the interests of national security.” The Department’s basic authorizing legislation for its personnel security program is codified in 5 U.S.C. 7531 – 5 U.S.C. 7533;
 - m. The Secure Embassy Construction and Counterterrorism Act of 1999 (Foreign Relations Authorization Act, FY 2000 and 2001, Title VI, Public Law 106-113), established two security requirements for U.S. diplomatic facilities abroad: collocation and setback. The authority to waive these requirements has been delegated to the Assistant Secretary for Diplomatic Security except for chancery and consulate buildings; and
 - n. Other authorities, as appropriate.

1 FAM 262 PRINCIPAL DEPUTY ASSISTANT SECRETARY FOR DIPLOMATIC SECURITY AND DIRECTOR OF THE DIPLOMATIC SECURITY SERVICE (DS/DSS)

(CT:ORG-344; 08-29-2014)

- a. The Principal Deputy Assistant Secretary (PDAS) for Diplomatic Security and Director of the Diplomatic Security Service (DS/DSS):
 - (1) Advises the Assistant Secretary for Diplomatic Security on the formulation and implementation of security programs and law enforcement policies for the Department and the foreign affairs community;
 - (2) Serves as the Director of the Diplomatic Security Service (DSS) and manages the day-to-day operations of the Department's security program at U.S. diplomatic and consular missions abroad;
 - (3) Directs personal protective services for the Secretary of State, other Department officials, certain resident foreign dignitaries, and dignitaries on official visits to the United States;
 - (4) Oversees the worldwide law-enforcement and protective-security responsibilities of the Diplomatic Security Service;
 - (5) Oversees the Department's personnel security program, which determines the issuance and maintenance of employee security clearances; and
 - (6) Chairs the Secretary's Overseas Security Advisory Council (OSAC), which promotes cooperation between U.S. business and private-sector interests abroad and the Department's security programs.
- b. The Principal Deputy Assistant Secretary for Diplomatic Security and Director of the Diplomatic Security Service also provides direct management oversight to the following:
 - (1) Directorate of the Deputy Assistant Secretary and Assistant Director of Countermeasures (DS/C):
 - (a) Office of Physical Security Programs (DS/C/PSP);
 - (b) Office of Security Technology (DS/C/ST); and
 - (c) Office of the Diplomatic Courier Service (DS/C/DC);
 - (2) Directorate of the Deputy Assistant Secretary and Assistant Director of International Programs (DS/IP):
 - (a) Office of Special Programs and Coordination (DS/IP/SPC);
 - (b) Office of Overseas Protective Operations (DS/IP/OPO); and
 - (c) Office of Regional Directors (DS/IP/RD);

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (3) Directorate of the Deputy Assistant Secretary and Assistant Director of High Threat Programs (DS/HTP):
 - (a) Office of Regional Directors (DS/HTP/RD); and
 - (b) Office of Special Programs (DS/HTP/SP).
- (4) Directorate of the Deputy Assistant Secretary and Assistant Director of Domestic Operations (DS/DO):
 - (a) Office of Domestic Facilities Protection (DS/DO/DFP);
 - (b) Office of Protection (DS/DO/P); and
 - (c) Office of Investigations and Counterintelligence (DS/DO/ICI);
- (5) Directorate of the Deputy Assistant Secretary and Assistant Director of Training (DS/T):
 - (a) Office of Antiterrorism Assistance (DS/T/ATA);
 - (b) Office of Training and Performance Standards (DS/T/TPS); and
 - (c) Office of Mobile Security Deployments (DS/T/MSD);
- (6) Directorate of the Deputy Assistant Secretary and Assistant Director of Threat Investigations and Analysis (DS/TIA):
 - (a) Office of Intelligence and Threat Analysis (DS/TIA/ITA);
 - (b) Office of Protective Intelligence and Investigations (DS/TIA/PII);
 - (c) Diplomatic Security Command Center (DS/TIA/CC); and
 - (d) Overseas Security Advisory Council (DS/TIA/OSAC).
- (7) Directorate of the Senior Coordinator for Security Infrastructure (DS/SI):
 - (a) Office of Information Security (DS/SI/IS);
 - (b) Office of Computer Security (DS/SI/CS); and
 - (c) Office of Personnel Security and Suitability (DS/SI/PSS);
- (8) Public Affairs (DS/PA).

1 FAM 262.1 Deputy Assistant Secretary and Assistant Director for Countermeasures (DS/C)

(CT:ORG-344; 08-29-2014)

The Deputy Assistant Secretary and Assistant Director for Countermeasures (DS/C):

- (1) Manages worldwide physical and technical security countermeasures programs);
- (2) Directs and provides management oversight to the:

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (a) Office of Physical Security Programs (DS/C/PSP);
 - (b) Office of Security Technology (DS/C/ST); and
 - (c) Office of the Diplomatic Courier Service (DS/C/DC);
- (3) Formulates security policy and program plans for worldwide physical and technical security countermeasures; and
- (4) Represents the Department in negotiations with other Federal agencies on issues regarding physical and technical security countermeasures;

**1 FAM 262.1-1 Office of Physical Security Programs
(DS/C/PSP)**

(CT:ORG-344; 08-29-2014)

The Office of Physical Security Programs (DS/C/PSP):

- (1) Directs and develops worldwide physical security standards, policies, procedures and guidelines for protecting personnel, facilities, and national security information of the Department and foreign affairs agencies;
- (2) Directs the implementation of physical security programs and ensures that Overseas Security Policy Board (OSPB) security standards and Department policies, procedures, and guidelines are met to protect diplomatic personnel, facilities, and information;
- (3) Develops and directs the implementation of the requirements of the Secure Embassy Construction and Counterterrorism Act of 1999 (22 U.S.C. 4865) mandating collocation and setback of U.S. diplomatic facilities abroad. DS/C/PSP provides an annual report to Congress on waivers granted by the Secretary and the Assistant Secretary for Diplomatic Security;
- (4) Develops and implements policies and procedures for certifying to Congress that appropriate action has been taken to protect all new office building construction and major renovation projects intended for the storage of classified materials or the conduct of classified activities;
- (5) Develops and directs the implementation of the construction security program to ensure that construction and other materials destined for controlled access areas at post facilities abroad are protected from acquisition to installation;
- (6) Directs the Research and Development Program to identify, evaluate, and recommend physical security countermeasures;
- (7) Directs activities of the Defensive Equipment and Armored Vehicle Division to ensure requirements for defensive and special protective equipment and armored vehicles are met;
- (8) Develops and directs the implementation of the domestic physical security programs, policies, procedures, and guidelines, and ensures that regulatory

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

requirements are met to protect Department personnel, facilities, and information throughout the United States; and

- (9) Directs activities of the Weapons of Mass Destruction Countermeasures Division to ensure training and equipment are provided to aid in surviving a chemical, biological, radiological, or nuclear attack.

1 FAM 262.1-1(A) Physical Security Division (DS/PSP/PSD)

(CT:ORG-233; 12-06-2010)

The Physical Security Division (DS/PSP/PSD):

- (1) Provides oversight to the Bureau of Overseas Buildings Operations (OBO) new office building (NOB) construction and major renovation projects to ensure compliance with OSPB security standards;
- (2) Evaluates NOB construction and major renovation projects and ensures the proper application of physical security and other standards in the selection, design, construction, and modification of buildings abroad to be occupied by the Department and foreign affairs agencies;
- (3) Certifies physical security equipment to meet specified performance criteria through in-house and independent testing;
- (4) Manages the development and installation of secure transit systems;
- (5) Performs physical security standards compliance inspections of new office buildings under construction by the Department; and
- (6) Prepares Congressional certifications with respect to the suitability of new U.S. embassies and consulates for classified operations and protection of personnel.

1 FAM 262.1-1(A)(1) Project Coordination Branch (DS/PSD/PCB)

(CT:ORG-254; 11-25-2011)

The Project Coordination Branch (DS/PSD/PCB):

- (1) Provides project evaluation to ensure proper application of physical security standards in the selection, design, construction, and modification of buildings abroad to be occupied by the Department and foreign affairs agencies;
- (2) Coordinates and ensures the adequacy and completeness of all requests for waiver of collocation and setback requirements of the Secure Embassy Construction and Counterterrorism Act of 1999 (SECCA) and/or exceptions to the OSPB security standards for all newly acquired facilities;
- (3) Provides input for and responds to requests from Congress, the Government Accountability Office, Office of the Inspector General, other

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

foreign affairs agencies, and Department bureaus and offices for information or guidance;

- (4) Provides technical review of RSO-recommended physical security upgrades at overseas schools and Department-sponsored recreation associations in support of the OBO-managed and funded Soft Target Program; and
- (5) Coordinates with OBO, members of the OSPB, and the Intelligence Community to ensure compliance with OSPB security standards.

1 FAM 262.1-1(A)(2) New Office Building Branch (DS/PSD/NOB)

(CT:ORG-233; 12-06-2010)

The New Office Building Branch (DS/PSD/NOB):

- (1) Provides project oversight to ensure that OSPB security standards and SECCA requirements are implemented for NOBs abroad. DS/PSD/NOB performs liaison/coordination functions for NOBs with OBO, the relevant diplomatic post, and other DS elements by actively tracking projects from the initial planning phase through final accreditation and move-in;
- (2) Is the key participant in site-selection surveys for all new embassy compounds (NECs);
- (3) Reviews all OBO project/design development plans for new construction;
- (4) Coordinates with the Intelligence Community to ensure technical, political violence, and terrorism threat security standards are met; and
- (5) Certifies physical security equipment (such as doors and barriers) that meet specified performance criteria (e.g., ballistic resistance, forced entry, and anti-ram) through in-house and independent testing.

1 FAM 262.1-1(A)(3) Certification, Accreditation, Transit Security Branch (DS/PSD/CAT)

(CT:ORG-233; 12-06-2010)

The Certification, Accreditation, Transit Security Branch (DS/PSD/CAT):

- (1) Recommends and implements construction security policies abroad;
- (2) Determines the appropriate level of construction security coverage abroad in accordance with OSPB construction security standards for all new office buildings (NOBs), major renovation/rehabilitation projects, and all construction projects occurring in the controlled access area (CAA) of diplomatic facilities abroad;
- (3) Recommends and implements policies and procedures for the certification of all such projects abroad in accordance with Section 160(a) of the

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (Public Law 100-204), as amended;

- (4) Recommends policies and develops procedures to ensure that construction and other materials destined for installations abroad are provided protection from the time of acquisition until installation;
- (5) Promotes the development of state-of-the-art secure transit systems and installation of the approved systems;
- (6) Conducts accreditation inspections of projects certified to Congress to ensure compliance with OSPB security standards, conformity with construction security plans, and proper operation of the security systems. Accreditation is required prior to occupancy and the processing and storage of classified information in the facility; and
- (7) Coordinates inspections programs, schedules, and objectives with OBO and other foreign affairs agencies.

1 FAM 262.1-1(B) Facilities Security Division (DS/PSP/FSD)

(CT:ORG-254; 11-25-2011)

The Facilities Security Division (DS/PSP/FSD):

- (1) Directs, manages, and provides oversight for physical security upgrades to Department facilities throughout the United States;
- (2) Develops domestic security policies, procedures, and guidelines for protecting Department personnel, facilities, and classified operations in accordance with the Department of Homeland Security (DHS) Interagency Security Committee standards;
- (3) Conducts security surveys and inspections of all Department domestic facilities to ensure compliance with Department policies and applicable Federal security guidelines;
- (4) Coordinates with the Bureau of Administration's Office of Operations (A/OPR), the General Services Administration (GSA), and commercial contractors to ensure that security installations are completed on schedule in compliance with domestic security policies, procedures, guidelines, and design specifications;
- (5) Coordinates funding with A/OPR, GSA, and commercial contractors for security systems and equipment, supporting infrastructure, secure procurement and storage, and construction surveillance technicians;
- (6) Provides security review of A/OPR domestic construction projects, relocations, and renovations of Department office spaces and facilities. DS/PSP/FSD designs security features for upgrades; prioritizes projects in consultation with A/OPR; and coordinates funding with requesting Department bureaus; and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (7) Evaluates and assesses Department and Department of Homeland Security (DHS) threat information for domestic facilities.

**1 FAM 262.1-1(B)(1) Project Coordination Branch
(DS/FSD/PCB)**

(CT:ORG-254; 11-25-2011)

The Project Coordination Branch (DS/FSD/PCB):

- (1) Directs, manages, and provides project management oversight for physical security upgrades to Department domestic facilities designated security Levels I through IV by the Department of Justice (DOJ);
- (2) Proposes improvements to physical security systems and equipment to ensure the protection of life, property, and information, while ensuring facility compliance with Department policies, procedures, and guidelines;
- (3) Coordinates with A/OPR and GSA on projects requiring the design and installation of security systems, such as proprietary alarms, automated access control, vehicle barrier systems, closed-circuit television, and high-security locking hardware;
- (4) Provides oversight for the development of memorandums of agreement (MOAs) for interagency transfer of support funds and tracking of the reimbursement of funds from other Department entities to ensure security project completion;
- (5) Provides construction security for security upgrades in sensitive areas of Department domestic facilities;
- (6) Reviews and assesses the results of security surveys and inspections of domestic facilities, including field and passport offices, regional centers, and DOJ-designated Level I through IV facilities. DS/FSD/PCB recommends cost-effective countermeasures to eliminate vulnerabilities and hazards and coordinates funding, prioritization, and drafts the statements of work to implement the installation of countermeasures;
- (7) Reviews Level I through IV A/OPR new construction and renovation projects of domestic office space and facilities; assists A/OPR in the prioritization of projects; and coordinates funding with the requesting Department bureau;
- (8) Designs and integrates intrusion-detection, access-control, closed-circuit television systems, and high-security locking hardware configurations in conjunction with security upgrades and office renovations;
- (9) Coordinates the inclusion of security requirements in the construction drawings and specifications with A/OPR, GSA, and commercial contractors; and
- (10) Tests and evaluates newly installed physical security equipment to ensure

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

compliance with Department security and operational requirements.

**1 FAM 262.1-1(B)(2) Domestic Buildings Branch
(DS/FSD/DBB)**

(CT:ORG-233; 12-06-2010)

The Domestic Buildings Branch (DS/FSD/DBB):

- (1) Designs the installation of intrusion-detection, access-control, and closed-circuit television systems, and high-security locking hardware for domestic facilities;
- (2) Provides oversight to ensure compliance with security requirements for major long-term technical and physical-security renovation projects at all DOJ-designated Level V Department facilities (Harry S Truman Building, Blair House, and U.S. Mission to the United Nations);
- (3) Coordinates the inclusion of security requirements in the construction drawings and specifications with A/OPR, GSA, and commercial contractors;
- (4) Provides classified drawings and specifications of facility renovations to construction project managers, coordinators, and construction surveillance technicians; and
- (5) Ensures commercial contractors comply with Department policies, procedures, and guidelines during construction.

**1 FAM 262.1-1(B)(3) Security Standards and Compliance
Branch (DS/FSD/SSC)**

(CT:ORG-233; 12-06-2010)

The Security Standards and Compliance Branch (DS/FSD/SSC):

- (1) Conducts evaluations, surveys, and inspections of Department domestic facilities to ensure compliance with Department policies, procedures, and guidelines;
- (2) Develops and maintains domestic security policies, procedures, and guidelines in concert with Interagency Security Committee standards for protecting Department personnel, facilities, and national security information;
- (3) Evaluates technical and terrorism threat information and vulnerabilities relating to domestic facilities;
- (4) Proposes improvements on the use of physical and technical security systems and certifies their use; and
- (5) Conducts quarterly alarm testing of the Department's classified processing areas to ensure compliance with policies, procedures, and guidelines.

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

1 FAM 262.1-1(C) Defensive Equipment and Armored Vehicle Division (DS/PSP/DEAV)

(CT:ORG-254; 11-25-2011)

The Defensive Equipment and Armored Vehicle Division (DS/PSP/DEAV):

- (1) Tests, evaluates, procures, and distributes defensive equipment worldwide;
- (2) Inspects DS-issued weapons to ensure they are functioning properly during DS agents' periodic requalification sessions at the DS Training Center;
- (3) Serves as the focal point for DS-issued weapons requiring repair or replacement;
- (4) Manages the armored vehicle program, which provides for the:
 - (a) Acquisition and secure shipment of all protective vehicles;
 - (b) Armoring of Department (Office of Logistics Management, Marine security guard, chief of mission) and International Cooperative Administrative Support Services (ICASS) security vehicles; and
 - (c) Procurement, product integrity, and worldwide deployment of the Department's armored vehicles; and
- (5) Represents the Department on international and U.S. Government interagency committees involved in developing uniform security standards for defensive equipment and armored vehicles.

1 FAM 262.1-1(D) Weapons of Mass Destruction Countermeasures Division (DS/PSP/WMD)

(CT:ORG-290; 10-31-2012)

The Weapons of Mass Destruction Countermeasures Division (DS/PSP/WMD):

- (1) Is responsible for providing weapons of mass destruction (WMD) countermeasures training and equipment to personnel under chief-of-mission authority to aid in surviving a chemical, biological, radiological, or nuclear attack;
- (2) Provides additional training and equipment abroad to first responders (volunteers approved at post for such service), local guards, bodyguards, surveillance detection personnel, and other designated security personnel;
- (3) Provides, in addition to the training abroad:
 - (a) Domestic WMD awareness training for personnel scheduled for assignment abroad;
 - (b) Escape mask training and equipment for Department employees assigned to designated State Department domestic facilities;
 - (c) Training for domestic and overseas mail handling and screening for

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

suspicious substances; and

- (d) Other WMD awareness and countermeasures training;
- (4) Researches and tests new WMD countermeasures equipment to ensure the equipment meets new or changing needs. DS/PSP/WMD plans procurements for deployment to Department facilities abroad and domestically; and
- (5) Represents DS on the Nuclear Trafficking Response Group (NTRG) and serves as the point of contact for the NTRG and regional security officers (RSOs) abroad in responding to NTRG concerns at overseas posts.

1 FAM 262.1-2 Office of Security Technology (DS/C/ST)

(CT:ORG-254; 11-25-2011)

The Office of Security Technology (DS/C/ST):

- (1) Provides management and policy direction to the Countermeasures Program Division (DS/ST/CMP), Security Technology Operations Division (DS/ST/STO), and Facility Security Engineering Division (DS/ST/FSE);
- (2) Directs the development of standards, policies, and procedures associated with technical countermeasures, TEMPEST, security technology operations, and facility security engineering programs domestically and abroad. DS/C/ST ensures that security standards for these disciplines are met to protect national security information, diplomatic facilities, and personnel abroad;
- (3) Directs the implementation of technical countermeasures, TEMPEST, security technology operations, and facility security engineering programs;
- (4) Develops and implements procedures to track facility profiles, post compliance with Overseas Security Policy Board (OSPB)-approved security technology standards, and exceptions to the OSPB standards;
- (5) Directs implementation of DS research and development programs to identify technical countermeasures and DS-approved technical security equipment. DS/C/ST fields approved technical security equipment and maintains an equipment lifecycle;
- (6) Represents the Department in intergovernmental and interagency organizations and specialized groups on matters relating to security technology programs; and
- (7) Coordinates all briefing papers and related materials concerning security technology programs abroad for DS and senior Department management; and
- (8) Directs programs that investigate and implement technical solutions that enhance life safety and security of personnel serving at overseas missions.

1 FAM 262.1-2(A) Countermeasures Program Division (DS/ST/CMP)

(CT:ORG-233; 12-06-2010)

The Countermeasures Program Division (DS/ST/CMP):

- (1) Provides management and policy direction to the Emanations Countermeasures Branch (DS/CMP/ECB), Technical Analysis Branch (DS/CMP/TAB), Technology Evaluation Branch (DS/CMP/TEB), and Technical Surveillance Countermeasures Branch (DS/CMP/TSC);
- (2) Provides Special Access Program (SAP) management;
- (3) Serves as the Department's voting member to the Technical Threat Working Group (TTWG);
- (4) Serves as the principal liaison to the foreign government members of the International Technical Security (INTECSEC) Group; and
- (5) Sponsors the INTECSEC security officer exchange program.

1 FAM 262.1-2(A)(1) Emanations Countermeasures Branch (DS/CMP/ECB)

(CT:ORG-344; 08-29-2014)

The Emanations Countermeasures Branch (DS/CMP/ECB):

- (1) Represents the Department on the National TEMPEST Advisory Group (TAG) to provide input for the development of national TEMPEST policy for U.S. Government agencies operating domestically and abroad;
- (2) Performs TEMPEST countermeasures reviews to determine TEMPEST countermeasures requirements domestically and abroad and performs TEMPEST inspections worldwide to ensure Department compliance with national emanations standards;
- (3) Manages DS' certified shielded enclosure (CSE), built-in conference room (BCR), and secure conference room (SCR) programs and provides preventive maintenance for DS-owned enclosures and conference rooms and certifies all shielded enclosures and conference rooms worldwide; and
- (4) Approves secret-level collateral secure video teleconferencing facilities abroad.

1 FAM 262.1-2(A)(2) Technical Analysis Branch (DS/CMP/TAB)

(CT:ORG-233; 12-06-2010)

The Technical Analysis Branch (DS/CMP/TAB):

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (1) Works with the Center for Security Evaluation to evaluate and implement a risk-management program designed to identify the specific countermeasures needed to protect classified and sensitive information;
- (2) Collects and analyzes information regarding technical threats to Department facilities abroad, security systems, and information systems;
- (3) Analyzes technical anomalies 24 hours a day, 7 days a week, at a security monitoring and analysis center (SMAC) located at the DS Command Center;
- (4) Provides input and representation to the Center for Security Evaluation through the TTWG to determine the level of technical threat and degree of risk to national security information at each U.S. diplomatic facility abroad;
- (5) Provides guidance, collection, and intelligence analysis of technical security assessments (TSAs), technical surveillance countermeasures (TSCMs), communications security (COMSEC) audits, and technical security reporting; and
- (6) Manages the COMSEC facility technical inspections program in accordance with the Foreign Affairs Manual (FAM), the Foreign Affairs Handbooks (FAHs), and national policy guidance.

**1 FAM 262.1-2(A)(3) Technology Evaluation Branch
(DS/CMP/TEB)**

(CT:ORG-233; 12-06-2010)

The Technology Evaluation Branch (DS/CMP/TEB):

- (1) Manages the security risk evaluation and approval process for the introduction of new information and telecommunications technology and equipment into the Department's facilities abroad; and
- (2) Reports on emerging technology trends and provides analysis pertinent to the Department.

**1 FAM 262.1-2(A)(4) Technical Surveillance Countermeasures
Branch (DS/CMP/TSC)**

(CT:ORG-233; 12-06-2010)

The Technical Surveillance Countermeasures Branch (DS/CMP/TSC):

- (1) Conducts global TSCM inspections in coordination with DS/ST/STO and DS/ICI/CI;
- (2) Serves as the Department's central coordinator for TSCM operations;
- (3) Manages TSCM programs and provides resources and services to reduce the risk of technical penetrations or technical hazards in Department

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

facilities domestically and abroad;

- (4) Ensures that all technical penetrations and technical hazards discovered at U.S. facilities abroad under the umbrella of the chief of mission are reported in coordination with DS/DO/ICI to the Directorate of Central Intelligence (DCI) in accordance with DCI Procedural Guides 1, 2, 3;
- (5) Ensures that all technical penetrations discovered at domestic Department facilities are reported in coordination with DS/DO/ICI to the Federal Bureau of Investigation; and
- (6) Provides centralized support for TSCM equipment, including procurement, inventory tracking, development, certification, and repair.

**1 FAM 262.1-2(B) Security Technology Operations Division
(DS/ST/STO)**

(CT:ORG-254; 11-25-2011)

The Security Technology Operations Division (DS/ST/STO):

- (1) Provides management and policy direction to the Naval Support Unit (DS/STO/NSU), the Overseas Support Branch (DS/STO/OSB), and the Security Engineering Services Branch (DS/STO/SES);
- (2) Directly supervises the OSB and SES branch chiefs and five regional directors for security engineering (RDSEs). RDSEs serve as field managers and the interface between DS, engineering services centers (ESCs), and engineering services offices (ESOs);
- (3) Manages and implements the Special Projects Program that uses technical solutions to enhance personnel life safety and security at designated locations. Program responsibilities include:
 - (a) Electronic countermeasures (ECM) to thwart radio frequency-activated improvised explosive devices;
 - (b) Mobile video systems (MVS) that provide event documentation for motorcades;
 - (c) Unmanned aero vehicles (UAV) that provide motorcade route surveillance and real-time situational awareness to the motorcade and technical operations center;
 - (d) Personnel locator and tracking (PLT) systems that provide location data and 911 capabilities for personnel conducting business outside the embassy. This capability supports personnel recovery and NSPD-12; and
 - (e) Sense and warn systems that detect and warn of indirect hostile fire; and
- (4) Includes associated operational support in tactical operations centers

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

(TOCs) and the DS command center as well as investigates and fields new safety and security technologies to meet evolving personnel protective needs.

1 FAM 262.1-2(B)(1) Naval Support Unit (DS/STO/NSU)

(CT:ORG-344; 08-29-2014)

The Naval Support Unit (DS/STO/NSU) supports the Department security engineering program abroad, and provides U.S. Navy Construction Battalion (Seabee) assets for DS and other U.S. Government projects under the terms of a memorandum of understanding (see 12 FAM Exhibit 451.5).

1 FAM 262.1-2(B)(2) Overseas Support Branch (DS/STO/OSB)

(CT:ORG-233; 12-06-2010)

The Overseas Support Branch (DS/STO/OSB):

- (1) Manages, coordinates, and supports the worldwide activities of technical security personnel abroad. These personnel are stationed in U.S. missions, in larger security engineering services centers (ESCs), or smaller engineering services offices (ESOs);
- (2) Prioritizes, obtains, coordinates, and disburses resources to support offices abroad, including positions, travel money, local operating funds, and vehicles;
- (3) Develops operational policy and procedures for technical security support;
- (4) Coordinates Naval Support Unit (NSU) security operations abroad;
- (5) Coordinates with regional directors in DS/IP, executive directors in regional bureaus, post management officers, desk officers in OBO/CFSM/SM, and others within the Department and in other agencies, on technical security operations and support abroad;
- (6) Prepares briefing materials for Office of Inspector General (OIG) recommendations on technical-security issues of an operational nature in conjunction with DS/MGT/PPD. Personnel may also participate in special project coordination and support as directed by DS management; and
- (7) Serves as the central repository for ESC/ESO reporting, to include technical security surveys and inspections.

1 FAM 262.1-2(B)(3) Security Engineering Services Branch (DS/STO/SES)

(CT:ORG-233; 12-06-2010)

The Security Engineering Services Branch (DS/STO/SES):

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (1) Performs TSCM inspections at domestic facilities;
- (2) Conducts sensitive compartmented information facility (SCIF) accreditation surveys in support of the Department's Special Security Operations Division (DS/IS/SSO);
- (3) Provides TSCM support for special missions and classified conferences;
- (4) Manages the technical security support program for the Secretary of State traveling mission. DS/STO/SES develops, procures, and deploys technical security equipment specifically for the Secretary of State support mission. DS/STO/SES coordinates among field offices to provide personnel, equipment, and technical security support for the Secretary of State when traveling abroad;
- (5) Provides technical security support for the protection of visiting dignitaries and international conferences, such as the United Nations General Assembly (UNGA), Economic Forum, and Peace Talks; and
- (6) Provides technical support to DS/DO/ICI in conducting criminal investigations.

**1 FAM 262.1-2(B)(4) Quality Assurance and Liaison Branch
(DS/STO/QAL)**

(CT:ORG-233; 12-06-2010)

The Quality Assurance and Liaison Branch (DS/STO/QAL):

- (1) Delivers systematic monitoring and evaluation services to OBO, DS/FSE/PME, DS/PSD/NOB, DS/PSD/CAT and others for Technical Security Systems (TSS) designs and installations. Quality assurance services include detailed quality audits, design reviews, standards development, and process improvement recommendations;
- (2) Conducts quality audits and reports discrepancies of TSS installation projects based upon statements of work (SOWs), regulations, and standards;
- (3) Facilitates the exchange of TSS information and ideas between DS and OBO, as well as with other Department domestic offices and missions abroad, and with other U.S. Government agencies;
- (4) Recommends process improvements supporting U.S. Government managers in their oversight of performance-based contracts by providing subject-matter experts and solutions to performance issues, preparing independent government cost estimates (IGCEs), and developing:
 - (a) Performance measures;
 - (b) Metrics;
 - (c) Standard operating procedures (SOPs);

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (d) Performance monitoring and quality assurance surveillance plans (QASPs); and
 - (e) Analysis of performance results and trends; and
- (5) Provides liaison and support for special projects as DS/C/ST directs.

1 FAM 262.1-2(C) Facility Security Engineering Division (DS/ST/FSE)

(CT:ORG-233; 12-06-2010)

The Facility Security Engineering Division (DS/ST/FSE):

- (1) Provides management and policy direction to the Domestic Management and Engineering Branch (DS/FSE/DME), Field Support Branch (DS/FSE/FSB), Project Management and Engineering Branch (DS/FSE/PME), and Technology Development Branch (DS/FSE/TDB); and
- (2) Verifies all DS-funded technical security systems are installed free of defect under existing DS installation standards and regulations.

1 FAM 262.1-2(C)(1) Domestic Management and Engineering Branch (DS/FSE/DME)

(CT:ORG-233; 12-06-2010)

The Domestic Management and Engineering Branch (DS/FSE/DME):

- (1) Provides maintenance and repair support for all Department technical security equipment installed domestically;
- (2) Manages the design, engineering, and installation of DS-approved facility security equipment as part of new technical security installations and technical security upgrades (TSUs) domestically. This includes coordination of project schedules and priorities, review and approval of technical designs, and development of bills of materials; and
- (3) Supports DS/STO/SES with technical security support for the Secretary of State residence, Presidential guesthouse, visiting dignitaries, and international conferences.

1 FAM 262.1-2(C)(2) Field Support Branch (DS/FSE/FSB)

(CT:ORG-233; 12-06-2010)

The Field Support Branch (DS/FSE/FSB):

- (1) Provides logistical support, including order processing, procurement, warehousing, shipment, and lifecycle management for technical security equipment worldwide; and
- (2) Reviews bills of material for the installation of technical security systems at

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

facilities where DS has security responsibility.

1 FAM 262.1-2(C)(3) Project Management and Engineering Branch (DS/FSE/PME)

(CT:ORG-233; 12-06-2010)

The Project Management and Engineering Branch (DS/FSE/PME):

- (1) Manages the design, engineering, and installation of DS-approved facility security equipment as part of new technical security installations and technical security upgrades (TSUs) abroad. This includes coordination of project schedules and priorities, review and approval of technical designs, development of bills of materials, coordination of funding, and collaboration with other offices;
- (2) Reviews bills of material for the installation of technical security systems developed by the engineering security center/engineering security office (ESC/ESO) and approved by the regional security officer (RSO), at facilities where DS has security responsibility; and
- (3) Verifies all technical security systems are installed free of defect under existing DS installation standards and regulations.

1 FAM 262.1-2(C)(4) Technology Development Branch (DS/FSE/TDB)

(CT:ORG-233; 12-06-2010)

The Technology Development Branch (DS/FSE/TDB):

- (1) Identifies, evaluates, develops, and approves technical security equipment;
- (2) Writes and publishes the Technical Security Installation Standards Handbook, Application and Installation Guidelines, and Technical Bulletins;
- (3) Provides technical assistance and guidance relating to DS-approved security systems; and
- (4) Reviews and updates technical security installation standards in the FAM/FAH.

1 FAM 262.1-3 Office of the Diplomatic Courier Service (DS/C/DC)

(CT:ORG-233; 12-06-2010)

The Office of the Diplomatic Courier Service (DS/C/DC):

- (1) Manages and administers the Diplomatic Courier Service and its four regional courier divisions located in Washington, DC, Miami, Frankfurt, and Bangkok, and its hub centers at Manama, Pretoria, Dakar, Seoul, Sao

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

Paulo, and Sydney;

- (2) Provides secure and expeditious transmission of classified and sensitive correspondence, equipment, and materials worldwide, in support of the Department and the foreign affairs community;
- (3) Formulates, coordinates, and implements policies, plans, and operational procedures for the Diplomatic Courier Service;
- (4) Provides liaison to the courier services of foreign governments, other nations, and international organizations;
- (5) Provides secure control and transport of unclassified but sensitive items or materials designated for use in construction projects abroad and nonconsumables for controlled-sensitive areas of U.S. embassies and consulates;
- (6) Oversees military support flights that deliver outsized courier material in support of worldwide regional posts; and
- (7) Operates the classified pouch vault and performs pouching functions traditionally assigned to the information programs center at some regional and hub locations where DS/C and the Bureau of Information Resource Management (IRM) concur.

1 FAM 262.2 Deputy Assistant Secretary and Assistant Director for International Programs (DS/IP)

(CT:ORG-344; 08-29-2014)

The Deputy Assistant Secretary and Assistant Director for International Programs (DS/IP):

- (1) Serves as the focal point within the Bureau of Diplomatic Security (DS) for coordinating international security programs;
- (2) Manages and directs the formulation, planning, coordination, policy development, and implementation of security programs that protect U.S. diplomatic missions;
- (3) Provides direct management oversight to the following International Programs elements:
 - (a) International Programs Resource Staff;
 - (b) Office of Regional Directors (DS/IP/RD);
 - (c) Office of Special Programs and Coordination (DS/IP/SPC); and
 - (d) Office of Overseas Protective Operations (DS/IP/OPO);
- (4) Manages high-profile security programs to include Embassy Local Guard Program, Emergency Action Planning, Worldwide Protective Services Program, Residential Security, coordination with Department of Defense

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

(DoD), Surveillance Detection, and the Marine Security Guard Program;

- (5) Formulates security policy and program plans for international operations;
- (6) Serves as the focal point for coordination of DS response to and participation in evacuation operations and international crises;
- (7) Represents the Department in negotiations with DoD on security issues abroad relating to DS/IP international programs and manages DoD security support to U.S. diplomatic missions and operations abroad; and,
- (8) Establishes the policy, coordination, and supervision requirements necessary to implement the MSG Program, in conjunction with DS/SPC/MSG, the Commanding Officer of Marine Corps Embassy Security Group (MCESG), and Assistant Deputy Commandant of the Marine Corps for Plans, Policies, and Operations (PP&O) (Security Division).

1 FAM 262.2-1 International Programs Resource Staff

(CT:ORG-344; 08-29-2014)

The International Programs Resource Staff is responsible for:

- (1) Supporting International Programs by developing and evaluating strategic plans, performance measures, and budgets for the Directorate.
- (2) The staff directs within the Directorate;
- (3) the flow of action, information, and decision documents such as Foreign Affairs Manual/Foreign Affairs Handbook (FAM/FAH), Office of Inspector General (OIG), Government Accountability Office (GAO), Overseas Security Policy Board (OSPB), and Special Equipment Review Board (SPERB) actions; and
- (4) The staff also integrates policy initiatives, organizational goals, and post and program requirements including staffing requirements, in conjunction with resource availability, and other duties as assigned.

1 FAM 262.2-2 Office of Regional Directors (DS/IP/RD)

(CT:ORG-344; 08-29-2014)

- a. The Office of Regional Directors (DS/IP/RD) is divided by geographic region into five regional directorates, each headed by a regional director, who reports to the Deputy Director of International Programs (IP). The regional directors are the primary liaison between DS and the Department's regional bureau executive directors, post management officers, and desk officers. The Deputy Director position serves as the Senior Operations Coordinator for International Programs and reports directly to the Deputy Assistant Secretary for DS/IP.
- b. The regional directorates are:
 - (1) Africa Region (DS/RD/AF);

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (2) Western Hemisphere Region (DS/RD/WHA);
- (3) East Asia and Pacific Region (DS/RD/EAP);
- (4) Europe and Eurasia Region (DS/RD/EUR); and
- (5) Near East and South and Central Asia Region (DS/RD/NEA-SCA);

c. Each regional director:

- (1) Serves as the primary point of contact within the Department and other U.S. Government agencies on security programs and activities at U.S. missions abroad;
- (2) Ensures that DS security programs and activities at posts abroad are responsive, effective, and conform with Department policy, regulations, and procedures;
- (3) Establishes priorities for all security programs abroad and coordinates the planning and review of security services at posts abroad;
- (4) Provides technical assistance to posts abroad and reviews and monitors post progress on individual security projects and programs; and
- (5) Coordinates all briefing papers and related materials concerning security programs abroad for DS and senior Department management.

1 FAM 262.2-3 Office of Special Programs and Coordination (DS/IP/SPC)

(CT:ORG-344; 08-29-2014)

DS/IP/SPCcoordinates:

- (1) the Marine Security Guard Program; and
- (2) Special Programs and Plans division, which includes:
 - (a) emergency action plans (EAPs);
 - (b) multiple liaison offices to DoD; and
 - (c) Bureau of Conflict and Stabilization Operations (CSO).

1 FAM 262.2-3(A) Marine Security Guard Staff (DS/SPC/MSG)

(CT:ORG-344; 08-29-2014)

The Marine Security Guard Staff (DS/SPC/MSG) manages the Marine Security Guard (MSG) Program for the Department, and maintains liaison with MCESG and the Assistant Deputy Commandant of the Marine Corps for PP&O (Security Division).

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

**1 FAM 262.2-3(B) Special Programs and Plans Division
(DS/SPC/SPP)**

(CT:ORG-344; 08-29-2014)

The Special Programs and Plans Division (DS/SPC/SPP) manages the following staffs and programs:

- (1) Emergency Planning Staff:
 - (a) Maintains 12 FAH-1 Emergency Planning Handbook, the principle source of guidance for posts to produce emergency action plans (EAPs). The staff provides supporting emergency planning guidance as necessary;
 - (b) Reviews posts' completed EAPs submitted through the Crisis and Emergency Planning Application (CEPA). The staff works with posts to make required changes or suggested improvements and approves and publishes EAPs; and
 - (c) Provides CEPA training to emergency action plan authors; and
- (2) Provides liaison officers to the DoD EUCOM, PACOM, and SOUTHCOM Geographic Combatant Commands;
- (3) Serves as liaison office for DoD Force Protection Detachments (FPD); and
- (4) Serves as primary DS liaison to CSO.

**1 FAM 262.2-4 Office of Overseas Protective Operations
(DS/IP/OPO)**

(CT:ORG-344; 08-29-2014)

The Office of Overseas Protective Operations (DS/IP/OPO):

- (1) Directs the development of Department standards, policies, and procedures for local guard, surveillance detection, residential security, and Worldwide Protective Services (WPS) programs at U.S. missions abroad;
- (2) Directs the implementation of local guard, surveillance detection, residential security, and WPS programs, and ensures that applicable Overseas Security Policy Board (OSPB) security standards and Department policies, procedures, and guidelines are met to protect diplomatic personnel, facilities, and residences abroad;
- (3) Directs the conduct of program management reviews to evaluate posts' management of local guard, residential security, surveillance detection, and WPS programs; and
- (4) Develops, maintains, and evaluates strategic plans, performance measures, budgets, and financial plans covering program responsibilities.

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

1 FAM 262.2-4(A) Facility Protection Division (DS/OPO/FPD)

(CT:ORG-344; 08-29-2014)

The Facility Protection Division (DS/OPO/FPD):

- (1) Provides administrative and operational management oversight for the Department's local guard, surveillance detection, and residential security programs implemented at U.S. missions abroad;
- (2) Contributes to the development of Department standards, policies, and procedures for local guard, surveillance detection, and residential security programs at U.S. missions abroad;
- (3) Assists in the review of local guard contract solicitations, contract modifications, and participates on technical evaluation panels that assist the source selection process;
- (4) Responds to post local guard, surveillance detection, and residential security funding requests and coordinates proper disbursement of program funds;
- (5) Assists post with program procurements, where applicable;
- (6) Conducts program management reviews of posts' local guard, surveillance detection, and residential security programs to ensure they are responsive, effective, and conform with Department standards and policy; makes recommendations to enhance the programs, tracks compliance; and
- (7) Maintains liaison with other foreign affairs and Intelligence Community agencies on local guard, surveillance detection, and residential security program matters.

1 FAM 262.2-4(B) Operational Support Division (DS/OPO/OSD)

(CT:ORG-344; 08-29-2014)

The Operational Support Division (DS/OPO/OSD):

- (1) Leads and guides the development of Department standards, policies, and procedures for local guard, surveillance detection, residential security, and Worldwide Protective Services programs at U.S. missions abroad;
- (2) Assists in acquisition planning, source selection, pre-award and post-award contract documentation, and invoicing for DS/IP/OPO programs;
- (3) Provides support to Contracting Officer's Representatives (CORs) worldwide in obtaining and maintaining FAC-COR certifications;
- (4) Coordinates financial and budgetary requirements, projections, and resource decisions with other functional and geographic bureaus, the DS Chief Financial Officer, and other elements of the Department and relevant

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

outside agencies in support of DS/IP/OPO programs;

- (5) Develops and implements analytics and other methodologies to identify and define problems, generate and evaluate alternatives, select options, manage risk, and evaluate programmatic, financial, and operational decisions; and
- (6) Supports the design, development, and maintenance of responsive suites of management information tools to optimize data availability and retrieval to aid program requirements analysis, validation, and evaluation, and to facilitate internal office, bureau, and Department management processes and accountability.

1 FAM 262.2-4(C) Worldwide Protective Services Division (DS/OPO/WPS)

(CT:ORG-344; 08-29-2014)

The Worldwide Protective Services Division (DS/OPO/WPS):

- (1) Contributes to the development of Department standards, policies, and procedures for the Worldwide Protective Services (WPS) program at designated U.S. missions abroad;
- (2) Executes the Department initiative to plan, organize, establish, deploy, and operate contractor-provided personal protection, guard, and support services at special conditions posts as defined in 12 FAM 057.3;
- (3) Coordinates with Department, DS program offices, regional security offices (RSOs), and military liaisons to ensure current WPS operations are sufficiently supported in logistical and operational matters;
- (4) Conducts program management reviews of posts' WPS programs to reinforce contract compliance and administrative procedures, and address deficiencies in performance or adherence to contract terms and conditions;
- (5) Assists in the review of WPS contract solicitations, modifications, and task orders, and participates on technical evaluation panels to support source selection;
- (6) Provides WPS contract oversight through WPS Division program officers serving as a COR or Government Technical Monitor (GTM) at post, and through DS Special Agents and Security Protective Specialists at post who have been designated as a COR; and
- (7) Directs the processing and certification for invoice payments submitted by contractors providing worldwide protective services.

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

1 FAM 262.3 Deputy Assistant Secretary and Assistant Director for High Threat Programs (DS/HTP)

(CT:ORG-344; 08-29-2014)

The Deputy Assistant Secretary and Assistant Director for High Threat Programs (DS/HTP):

- (1) Reports to the Assistant Secretary of Diplomatic Security on matters related to the direct support of U.S. diplomatic missions and consulates identified in the HTP portfolio. On routine and administrative matters the DAS for DS/HTP will report to the PDAS for all other routine and administrative matters;
- (2) Serves as the focal point within DS for coordinating security programs at the designated HTP posts;
- (3) Manages and directs the formulation, planning, coordination, policy development, and implementation of security programs that protect U.S. diplomatic missions in the HTP portfolio;
- (4) Provides direct management oversight to the following High Threat Programs elements:
 - (a) Office of Regional Directors (DS/HTP/RD); and
 - (b) Office of Special Programs (DS/HTP/SP).
- (5) Manages high-profile security programs to include personnel recovery, tactical and strategic planning, special operations, coordination with Department of Defense (DoD), Security Protective Specialists;
- (6) Serves as the focal point for coordination of DS response to and participation in evacuation operations and international crises at HTP posts;
- (7) Represents the Department in negotiations with DoD on security issues abroad relating to DS/HTP programs; and
- (8) Coordinates DoD security support to U.S. diplomatic missions and operations and coordinates extraordinary U.S. Marine Corps (USMC) support to the HTP posts with the Commander Marine Corps Embassy Security Group.

1 FAM 262.3-1 Office of Regional Directors (DS/HTP/RD)

(CT:ORG-344; 08-29-2014)

- a. The Office of Regional Directors (DS/HTP/RD) is divided by geographic region into three HTP regional directorates; each is headed by a regional director who reports to the Office Director of the Office of Regional Directors, High Threat Programs (HTP). The regional directors are the primary liaison between DS and the Department's regional bureau executive directors, HTP post management officers, and HTP desk officers. The Office Director position reports directly to

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

the Deputy Assistant Secretary for DS/HTP.

- b. The regional and functional directorates are:
 - (1) Africa Region (DS/HTP/RD/AF);
 - (2) Near East Asia and South and Central Asia Region (DS/HTP/RD/NEA-SCA); and
 - (3) Iraq and Afghanistan (DS/HTP/RD/IA).
- c. Each regional or functional director:
 - (1) Serves as the primary point of contact within the Department and other U.S. Government agencies on security programs and activities at U.S. missions abroad in the HTP portfolio;
 - (2) Ensures that DS security programs and activities at HTP posts abroad are responsive, effective, and conform with Department policy, regulations, and procedures;
 - (3) Establishes priorities for all security programs abroad and coordinates the planning and review of security services at HTP posts abroad;
 - (4) Provides technical assistance to HTP posts abroad and reviews and monitors post progress on individual security projects and programs; and
 - (5) Coordinates all briefing papers and related materials concerning security programs abroad for DS and senior Department management.
- d. The Office of Regional Directors coordinates with HTP posts to facilitate and ensure implementation and compliance with Interagency Security Assessment Team (ISAT) recommendations until all ISAT recommendations are either completed or closed out.

1 FAM 262.3-2 Office of Special Programs (DS/HTP/SP)

(CT:ORG-344; 08-29-2014)

The Office of Special Programs (DS/HTP/SP):

- (1) Coordinates the Personnel Recovery program for U.S. missions abroad;
- (2) Provides representation and expertise in response to crisis situations, including Department task forces and security support teams;
- (3) Develops, implements, and codifies future operations plans and fosters innovative operational thinking in support of the Bureau of Diplomatic Security;
- (4) Administratively supports protective security operations of designated posts through management and administration of the Security Protective Specialist (SPS) program;
- (5) Ensures effective communication and coordination with HTHR-related U.S. military commands through management of liaison officers; and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (6) Manages, administers, and oversees the Bureau of Diplomatic Security's Explosive Ordnance Disposal (EOD) program for specific HTP posts.

1 FAM 262.3-2(A) Special Operations Unit

(CT:ORG-344; 08-29-2014)

- a. The Special Operations Unit is responsible for coordination between:
- (1) the Department of State (DOS);
 - (2) the Department of Defense (DoD); and
 - (3) the component commands.
 - (a) e.g., Unified (UCC);
 - (b) Geographic (GCC);
 - (c) Central Command (CENTCOM);
 - (d) Africa Command (AFRICOM);
 - (e) Joint (JSOC), and
 - (f) Special Operations (SOCOM) for:
 - (i) emergency planning and response;
 - (ii) security assistance; and
 - (iii) associated support to U.S. diplomatic missions.
- b. The Unit provides Department representation and specialized expertise in response to:
- (1) crises;
 - (2) task forces; and
 - (3) emergency security support teams to include:
 - (a) operational and training elements of the DoD;
 - (b) interagency community, and
 - (c) perform other duties and tasks as assigned.
- c. The Unit synchronizes with specialized U.S. military support to respond to critical incidents through strategic planning, integrated surveys, coordination and implementation. The Unit has global responsibilities in support of all U.S. diplomatic missions.

1 FAM 262.3-2(B) Operations Planning Unit

(CT:ORG-344; 08-29-2014)

- a. The Operations Planning Unit is responsible for creating comprehensive, integrated, and innovative solutions to complex Bureau-level operational

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

planning requirements using a deliberate planning process and available intra- and interagency subject matter expertise.

- b. The Unit manages and maintains a central repository of the Bureau's operations plans, institutionalizes a deliberate planning process for Bureau-wide operations planning, identifies captures, evaluates, and institutionalizes operational lessons learned to improve DS operations at the tactical, operational, and strategic levels, and other duties as assigned.

1 FAM 262.3-2(C) High Threat Programs Resource Unit

(CT:ORG-344; 08-29-2014)

The High Threat Programs Resource Unit is responsible for developing, maintaining and evaluating budgets and financial data for the Directorate, including the annual program and project plans for incorporation into the Bureau Resource Request (BRR). The Unit may also assist those charged by the DAS for DS/HTP with the coordination of information or action concerning decision documents such as FAM/FAH, OIG, GAO, OSPB, SPERB and ARB actions, ensuring coordination and completion for the Deputy Assistant Secretary for DS/HTP, and other duties as assigned.

1 FAM 262.4 Deputy Assistant Secretary and Assistant Director for Domestic Operations (DS/DO)

(CT:ORG-344; 08-29-2014)

The Deputy Assistant Secretary and Assistant Director for Domestic Operations (DS/DO):

- (1) Oversees criminal investigations domestically and abroad, related to threats against Department personnel, facilities, and visiting foreign dignitaries;
- (2) Oversees and manages investigations of Department-related passport and visa violations, both domestically and abroad, implementing DS' Visa and Passport Strategic Plan;
- (3) Oversees and manages counterintelligence-related investigations, maintaining relationships with the Intelligence Community and other law enforcement organizations;
- (4) Represents senior management interests to Federal, State, and local law enforcement agencies and departments;
- (5) Oversees investigations of allegations of malfeasance, misfeasance, and nonfeasance related to Department personnel, and conducts investigations into criminal and administrative misconduct involving personnel, contractors, and dependents at posts abroad and domestically;
- (6) Oversees the management of the Assistant Regional Security Officer

1 FAM 260 Page 32 of 81

UNCLASSIFIED (U)

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

Investigator Program, coordinating efforts with the Bureau of Consular Affairs;

- (7) Assigns DS agents to the Immigration and Customs Enforcement led by document benefits fraud task forces across the United States;
- (8) Oversees investigations of use-of-force incidents involving Department employees and contractors;
- (9) Oversees and manages a network of eight domestic field offices and 22 resident offices that carry out DS's criminal investigative missions throughout the United States;
- (10) Serves as DS's regional liaison, through its domestic offices, with Federal and local law enforcement, foreign mission personnel (with regard to security matters), local officials, and the private sector;
- (11) In cooperation with DS/TIA/PII, manages DS representation to joint terrorism task forces (JTTFs) by directly supervising agents assigned to regionally-based JTTFs throughout the United States;
- (12) Oversees the protection of the Secretary of State, along with the U.S. Ambassador to the United Nations, foreign dignitaries, and other persons of interest, as assigned;
- (13) Oversees the security, protective operations, and U.S. Government law enforcement and security coordination for international athletic events with official U.S. representation;
- (14) Oversees and manages a coordinated system combining state-of-the-art technical security equipment, physical security measures, and uniformed officers that protect personnel, information, and property at the Department's domestic facilities; and
- (15) Coordinates with other DS directorates using an existing matrix of robust security policies, procedures, technical and operational security programs and counterintelligence capabilities to address insider threat tasks and functions as prescribed by the National Insider Threat Policy and corresponding minimum standards, especially regarding network user monitoring, security auditing, incident handling, and supporting counterintelligence investigative matters. Additionally, provides security awareness training materials to all cleared personnel to enhance their awareness of insider threat issues, including threat indicators, threat methods and mandatory reporting requirements.

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

1 FAM 262.4-1 Office of Investigations and Counterintelligence (DS/DO/ICI)

(CT:ORG-344; 08-29-2014)

The Office of Investigations and Counterintelligence (DS/DO/ICI), Oversees the development and direction of a wide range of investigative programs and activities, including:

- (a) Investigations of passport and visa issuance and use;
- (b) Counterintelligence (CI) investigations;
- (c) Investigations and security assistance to other U.S. Government agencies;
- (d) Liaison with INTERPOL;
- (e) Other special investigations; and
- (f) Provides assistance through the Victims' Resource Advisory Program (VRAP) to those victimized as a result of crimes investigated by DS.;

1 FAM 262.4-1(A) Counterintelligence and Counterterrorism Vetting Unit

(CT:ORG-344; 08-29-2014)

The Counterintelligence and Counterterrorism Vetting Unit reports to the Director, Office of Investigations and Counterintelligence, and is responsible for vetting candidates for hire and assignment to sensitive positions at contingency operations or special-conditions posts. The Counterintelligence and Counterterrorism Vetting Unit:

- (1) queries Intelligence Community and law enforcement records maintained in databases with restricted access;
- (2) provides an analytical review of the security files of personnel whose backgrounds or assignments trigger supplemental review due to CI or CT concerns;
- (3) conducts checks on behalf of regional security officers clearing locally engaged staff; and
- (4) manages the DS polygraph program in accordance with 12 FAM 250 and 12 FAM 422.5.

1 FAM 262.4-1(B) Criminal Investigations Division (DS/ICI/CR)

(CT:ORG-344; 08-29-2014)

The Criminal Investigations Division (DS/ICI/CR):

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (1) Coordinates investigative complaints, allegations, information, and unusual incidents involving Department employees and all U.S. Government personnel under chief-of-mission authority;
- (2) Is responsible for the administrative and operational case control of crimes associated with passport and visa issuance and use;
- (3) Is responsible for administrative and operational case control of criminal investigations, as authorized by law and regulations;
- (4) Coordinates with the Office of Inspector General (OIG) and other Federal, State, and local law enforcement entities when it appears that violations of law or regulations have occurred for which they have investigative authority; and
- (5) Conducts and/or coordinates:
 - (a) Criminal investigation leads for other Federal, State, and local agencies, as requested;
 - (b) Criminal investigation leads on U.S. Government personnel under chief-of-mission authority; and
 - (c) Special criminal investigations and inquiries.

1 FAM 262.4-1(C) Counterintelligence Division (DS/ICI/CI)

(CT:ORG-344; 08-29-2014)

The Counterintelligence Division (DS/ICI/CI):

- (1) Develop and directs the Department's worldwide counterintelligence (CI) program;
- (2) Monitor, identify, and neutralize foreign intelligence efforts directed against Department and U.S. mission facilities and personnel;
- (3) Conducts substantive CI investigations and inquiries of:
 - (a) Allegations of espionage;
 - (b) Technical penetration of U.S. missions abroad;
 - (c) Developmental targeting;
 - (d) Foreign intelligence services recruitment and recruitment attempts;
 - (e) Exploitable conduct of U.S. Government employees;
 - (f) Suspect activities involving Foreign Service nationals (FSNs); and
 - (g) Other matters relevant to CI investigations.
- (4) Conducts CI screening of Department personnel and contractors being assigned to critical intelligence-threat countries or when background indicators require special CI attention; and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (5) Provides Department personnel with CI awareness training; coordinates the CI working groups for posts abroad; conducts CI analyses; directs the CI Assistance Program; and performs CI liaison for the Department.

**1 FAM 262.4-1(D) Special Investigations Division
(DS/ICI/SID)**

(CT:ORG-344; 08-29-2014)

The Special Investigations Division (DS/ICI/SID):

- (1) Conducts investigations into criminal and administrative misconduct involving personnel, contractors, and dependents at posts abroad;
- (2) Conducts investigations into administrative misconduct committed by Department employees and contractors stationed domestically; and
- (3) Conducts investigations in situations such as the following:
 - (a) Cases that involve child abuse and/or child neglect;
 - (b) Death investigations to include homicide, suicide, and unattended deaths of persons under chief-of-mission authority;
 - (c) Investigations into work place violence incidents determined as criminal in nature;
 - (d) Investigations of violations of the Military Extraterritorial Jurisdiction Act that have a nexus to Department equities;
 - (e) Sexual assault;
 - (f) Unauthorized disclosure of classified or other sensitive information;
 - (g) Substance abuse;
 - (h) Financial misconduct;
 - (i) Discharge of a firearm and/or use of force;
 - (j) Loss of credentials and/or identification pins and/or special protective equipment;
 - (k) Abuse of diplomatic pouch;
 - (l) Missing employees;
 - (m) Sexual misconduct (only in cases where such conduct has prejudicial potential to the U.S. Government, makes the employee vulnerable to coercion, or places the employee or others in physical danger);
 - (n) Spousal abuse involving employees assigned abroad; and
 - (o) Other cases involving employees' suitability and other violations of Department policies related to the Standards of Conduct; and
- (3) Representing the Bureau of Diplomatic Security at the Department's Family

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

Advocacy Committee; and

- (4) Conducts and coordinates:
 - (a) Special criminal investigations and inquiries; and
 - (b) Investigations that the Office of Inspector General (OIG) refers to DS.

1 FAM 262.4-1(E) Computer Investigations and Forensics Division (DS/ICI/CIF)

(CT:ORG-344; 08-29-2014)

The Computer Investigations and Forensics Division (DS/ICI/CIF) provides investigative support to the Department, including unique technical capabilities such as digital forensic analysis, cyber investigations, technical surveillance equipment, and operational support. DS/ICI/CIF is organized into three programs:

- (1) Computer Investigations Program:
 - (a) Investigates cyber crimes that target the Department or are perpetrated through the Internet or other electronic networks;
 - (b) Carries out related law enforcement and other security functions for the Department; and
 - (c) Provides investigative support to all elements of the Department in the seizure or collection of digital, electronic, or computer-related evidence from all kinds of electronic devices such as computers, camera systems, cell phones, and mobile devices;
- (2) The Digital Forensics Program provides forensic laboratory support (i.e., collection, preservation, analysis, explanation, presentation, and litigation support) as it relates to digital, electronic, cellular, audio, or video evidence; and
- (3) The Technical Surveillance Program provides technical surveillance equipment, specialized operational support, and related training to DS investigators and staff.

1 FAM 262.4-2 Office of Domestic Facilities Protection (DS/DO/DFP)

(CT:ORG-344; 08-29-2014)

The Office of Domestic Facilities Protection (DS/DO/DFP):

- (1) Manages the operational security and security support programs for all Department domestic facilities;
- (2) Is responsible for the protection of personnel, information, and property at all Department domestic facilities;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (3) Directs the Uniformed Protection and Security Support divisions;
- (4) Represents the Department on the Interagency Security Committee and other applicable interagency groups for domestic security;
- (5) Serves as the Department's primary point of contact for Federal, State, local government, and law enforcement agencies related to domestic facility security and protection matters;
- (6) Develops and implements domestic security standards, policies, and guidelines; and
- (7) Coordinates all domestic security delegations of authority with the General Services Administration, Department of Homeland Security/Federal Protective Service or other entities as appropriate.

1 FAM 262.4-2(A) Uniformed Protection Division (DS/DFP/UPD)

(CT:ORG-344; 08-29-2014)

The Uniformed Protection Division (DS/DFP/UPD):

- (1) Manages the uniformed protective services guard contracts and oversees guard services at all Department domestic facilities;
- (2) Manages and operates the domestic Security Control Center;
- (3) Manages uniformed security officers for the Diplomatic Security Service's (DSS) protective operations;
- (4) Provides access and property control at domestic facilities;
- (5) Provides domestic site security for the Department's Secretariat;
- (6) Coordinates and determines security needs for all domestic classified and unclassified conferences, special events, or special access;
- (7) Provides security and operational oversight for large-scale domestic special events;
- (8) Provides security oversight for domestic facility emergency action plans and input to all domestic occupant emergency plans; and
- (9) Manages or coordinates the appropriate response to security-related emergency situations (e.g., fires, bomb threats, suspicious packages, and security alarms) in all domestic Department facilities.

1 FAM 262.4-2(B) Security Support Division (DS/DFP/SSD)

(CT:ORG-344; 08-29-2014)

The Security Support Division (DS/DFP/SSD):

- (1) Is responsible for building pass identification issuance; security systems

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

administration; Domestic Security Officer's Program; and Domestic Facilities Protection (DS/DO/DFP) budget, policy, and procedural development and implementation;

- (2) Manages the DSS Identification Media Program that develops and issues ID cards, DSS credentials, badges, and security pins;
- (3) Manages the Diplomatic Security Identification Service (DSIS) Program that develops and issues all Department building pass identification cards (BPICs) in compliance with Federal Information Processing Standard Publication (FIPS PUB) 201 standards and associated special publications;
- (4) Provides customer support for building pass ID media and alarm-system operations;
- (5) Provides security briefings for procedural security requirements, security awareness, and violence in the workplace;
- (6) Provides access history for employee or visitor ingress and egress to internal or external law enforcement and other authorized entities;
- (7) Manages the Intelligence Community Badge Program in coordination with the Bureau of Intelligence and Research (INR);
- (8) Provides employee training for the operation of access control systems/media and alarm systems;
- (9) Manages the domestic Lock and Key Program, which maintains inventories and authorizes issuance of all security keys and locks in coordination with other DS offices, the Bureau of Administration (A), and the Department's lock contractor;
- (10) Offers a crime prevention program for all Department employees; and
- (11) Reports and coordinates theft investigations with the Office of Inspector General (OIG) or other law enforcement organizations, as appropriate.

1 FAM 262.4-3 Office of Protection (DS/DO/P)

(CT:ORG-344; 08-29-2014)

The Office of Protection (DS/DO/P):

- (1) Manages and directs protective security for the Secretary of State, other official representatives of the United States and foreign governments, and Department protective liaison programs;
- (2) Manages and coordinates the protection of certain foreign missions and officials in the United States; and
- (3) Administers reimbursements to Federal, State, and local law enforcement agencies or private security companies for expenses incurred in the protection of certain foreign government and United Nations missions and officials.

UNCLASSIFIED (U)

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

1 FAM 262.4-3(A) Dignitary Protection Division (DS/P/DP)

(CT:ORG-344; 08-29-2014)

The Dignitary Protection Division (DS/P/DP):

- (1) Coordinates protective services to visiting foreign dignitaries, resident foreign officials, and U.S. Government officials;
- (2) Organizes and manages protective services for special events involving multiple protectees; and
- (3) Coordinates with the U.S. Secret Service and other Federal, State, and local law enforcement agencies or private security companies involved with protective security.

1 FAM 262.4-3(B) Protective Liaison Division (DS/P/PL)

(CT:ORG-344; 08-29-2014)

The Protective Liaison Division (DS/P/PL):

- (1) Maintains liaison with appropriate U.S. Government agencies, foreign governments, Federal, State, and local law enforcement agencies, or private security companies assisting the Department with protective security;
- (2) Coordinates and monitors State and local police protection for certain foreign missions;
- (3) Provides information and assists foreign missions with security threats and offers guidance on the security aspects of diplomatic and consular immunity; and
- (4) Administers the reimbursement of funds to Federal, State, and local law enforcement agencies or private security companies that provide extraordinary protective services to certain resident foreign officials, facilities, and visiting foreign government officials.

1 FAM 262.4-3(C) Secretary's Detail (DS/P/SD)

(CT:ORG-344; 08-29-2014)

The Secretary's Detail (DS/P/SD) provides protection for the Secretary of State and immediate family, as well as comprehensive security coverage of the Secretary's residence.

1FAM 262.4-3(D) Major Events Coordination Unit

(CT:ORG-344; 08-29-2014)

The Major Events Coordination Unit (MECU) reports to the Director, Office of Protection, and coordinates U.S. Government resources leading up to and during

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

major international events that have significant U.S. Government participation.
The unit:

- (1) Serves primarily in a protective liaison and advisory capacity as the interagency security and law enforcement lead for major events abroad through the leadership of the 20-plus agencies represented on the International Security Events Group under the authorities of National Security Presidential Directive 46;
- (2) Assists with the long-range coordination of major international events and provides RSOs or designated security coordinators with guidance on event planning;
- (3) Coordinates with intelligence, law enforcement, security, diplomatic, crisis management, and host/organizing communities to ensure an efficient, appropriate, and comprehensive U.S. Government resources portfolio that is prepared to address potential security issues at major events worldwide in addition to other duties as assigned; and
- (4) Provides information and assists foreign host-country governments and appropriate entities in countering security threats—especially those threats potentially impacting U.S. interests leading up to and during major international events.

1 FAM 262.4-4 Office of Field Office Management (DS/DO/FLD)

(CT:ORG-344; 08-29-2014)

Oversees and directs the operation of all domestic DS field and resident agent offices:

- (a) Performs criminal investigations of passport and visa issuance and/or use crimes, and, in coordination with and direction from DS/TIA/PII, conducts protective intelligence investigations;
- (b) Serves on law enforcement task forces where there is a nexus to passport and visa crimes and/or when such service is in support of the DSS investigative, protective, or liaison mission;
- (c) Protects the Secretary of State, foreign dignitaries, resident foreign officials, and other persons under the authority of the U.S. code;
- (d) Provides protective and security-related liaison with foreign diplomatic and consular missions located within the geographic region of the field offices;
- (e) Performs liaison functions with local and Federal law enforcement agencies for the purpose of information and intelligence sharing;
- (f) Facilitates investigative efforts of the Office of Inspector General (OIG), as referred by DS headquarters; and
- (g) Provides protective security and operational support to U.S. Embassies

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

and Consulates in times of increased threat and operational need.

1 FAM 262.5 Deputy Assistant Secretary and Assistant Director for Training (DS/T)

(CT:ORG-344; 08-29-2014)

The Deputy Assistant Secretary and Assistant Director for Training (DS/T):

- (1) Advises the Principal Deputy Assistant Secretary and Director of the Diplomatic Security Service on the formulation and implementation of all security and law enforcement training programs and policies for the Bureau of Diplomatic Security;
- (2) Manages a directorate comprised of the Office of Antiterrorism Assistance, the Office of Training and Performance Standards, and the Office of Mobile Security Deployments;
- (3) Oversees the development, training, and coordination of related equipment and assistance to foreign government security and law enforcement personnel to deter and counter terrorism;
- (4) Directs the development and implementation of training courses to provide specialized training in technical security;
- (5) Directs the formulation, coordination, and implementation of security and law enforcement training programs that promote the professional development of DS personnel; and
- (6) Oversees the specialized training at Foreign Service (FS) posts on security topics on a regular and emergency basis, and provides emergency security support to posts abroad during periods of high threat, crisis, or natural disaster.

1 FAM 262.5-1 Office of Antiterrorism Assistance (DS/T/ATA)

(CT:ORG-344; 08-29-2014)

The Office of Antiterrorism Assistance (DS/T/ATA) is the primary implementer of foreign assistance antiterrorism training abroad. It:

- (1) Provides training and related donor equipment and assistance to enhance the ability of foreign government law enforcement and supporting security personnel to detect, deter, and investigate counterterrorism;
- (2) Strengthens the bilateral ties of the United States by developing training programs in coordination with selected U.S. mission country teams and host governments to provide an efficient and effective means of deterring and countering terrorism through modern humane techniques and practices; and
- (3) Coordinates training and assistance with the Office of the Coordinator for

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

Counterterrorism (S/CT), the Bureau of Democracy, Human Rights, and Labor (DRL), the Bureau of International Narcotics and Law Enforcement Affairs (INL), geographic bureaus, and other agencies, departments, and organizations.

1 FAM 262.5-1(A) Assessment, Review and Evaluation Staff (DS/ATA/ARE)

(CT:ORG-344; 08-29-2014)

The Assessment, Review, and Evaluation Staff:

- (1) Conducts initial capabilities assessments of partner nation (PN) law enforcement and security organizations, based on a defined set of program measure-of-effectiveness (PME) core criteria to be used as the basis for formulation of country assistance plans (CAPs);
- (2) Conducts periodic program reviews of PN law enforcement and security organizations to assess changes in capabilities and evaluate the effectiveness of antiterrorism assistance (ATA); and
- (3) Assesses the level of PN law enforcement and security organizations to internalize and sustain anti-terror capabilities developed with ATA, and makes recommendations on the inclusion of sustainment activities in CAPs.

1 FAM 262.5-1(B) Resources, Budget and Support Staff - (DS/ATA/RBS)

(CT:ORG-344; 08-29-2014)

The Resources and Support Staff:

- (1) Maintains internal controls over financial allocations and allotments and prepares background for Congressional Notifications in support of ATA;
- (2) Provides budget and financial reporting including reconciliation and financial oversight for all global and bilateral ATA programs;
- (3) Provides logistical support for ATA courses and equipment grants worldwide; and
- (4) Procures and maintains controlled defense articles and services in accordance with International Traffic in Arms Regulations (ITAR) and Department of Commerce instructions.

1 FAM 262.5-1(C) Training Curriculum Division (DS/ATA/TCD)

(CT:ORG-344; 08-29-2014)

The Training Curriculum Division (DS/ATA/TCD):

- (1) Oversees all aspects of the ATA training curriculum from course design

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

through implementation, incorporating accepted law enforcement and security practices, adult learning principles, and the institutionalization of human rights practices in partner nations;

- (2) Evaluates course form and content, and designs an evaluation program of student learning; and
- (3) Maintains a regular cycle for review and updates of all ATA curriculums.

1 FAM 262.5-1(D) Training Delivery Division (DS/ATA/TDD)

(CT:ORG-344; 08-29-2014)

The Training Delivery Division (DS/ATA/TDD):

- (1) Implements the worldwide delivery of all ATA training and consultation activities in accordance with individual country assistance plans (CAPs);
- (2) Initiates all instructional, administrative, and logistical preparations and coordination in support of training activities; and
- (3) Reviews each program of instruction (POI) as it relates to field experiences and provides updated curriculum recommendations to DS/ATA/TCD.

1 FAM 262.5-1(E) Training Management Division (DS/ATA/TMD)

(CT:ORG-344; 08-29-2014)

The Training Management Division (DS/ATA/TMD):

- (1) Manages bilateral and regional ATA operations, budgeting, activity scheduling, coordination, planning and reporting, country consultations and visits, and monitors both training results and resource accountability;
- (2) Develops individual CAPs with U.S. embassies for each partner nation (PN), based on a formal assessment of capacities and capabilities; and
- (3) Guides the progress of ATA to each PN starting when a memorandum of intent or other arrangement/agreement is reached.

1 FAM 262.5-2 Office of Training and Performance Standards (DS/T/TPS)

(CT:ORG-344; 08-29-2014)

The Office of Training and Performance Standards (DS/T/TPS):

- (1) Formulates, coordinates, and implements programs that promote the training and professional development of DS personnel;
- (2) Provides specialized security training for other employees of the Department and foreign affairs agencies and their eligible family members;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (3) Assists in training local, State, and other Federal law enforcement personnel;
- (4) Provides analysis, design, development, and evaluation to support standardization and accreditation of applicable DS training programs;
- (5) Provides leadership and management initiatives, training newsletters, and professional video services to augment existing training programs and expand the professional development opportunities available to DS employees; and
- (6) Provides a full range of administrative support services to include procurement actions, audiovisual services, budgeting, external training, preparing the DS Training Catalog, maintaining student-training records, registrar services, and building maintenance oversight.

1 FAM 262.5-2(A) Security and Law Enforcement Training Division (DS/TPS/SLTD)

(CT:ORG-344; 08-29-2014)

The Security and Law Enforcement Training Division (DS/TPS/SLTD):

- (1) Develops courses and provides instruction and course coordination for:
 - (a) Basic Special Agent training;
 - (b) Basic Regional Security Officer training;
 - (c) Special Agent In-Service training;
 - (d) Regional Security Officer In-Service training; and
 - (e) High-Threat Tactical Training;
- (2) Develops specialized training courses and provides instruction of these courses to DS and other personnel to meet DS's global mission requirements;
- (3) Provides subject-matter expertise for the Security Overseas Seminar to include briefings on surveillance detection and explosives recognition;
- (4) Provides specific security training to chiefs of mission (COMs), deputy chiefs of mission (DCMs), principal officers, post security officers, and Foreign Service national investigators (FSNIs); and
- (5) Provides specialized training in security subjects, such as weapons, defensive tactics/room entry, counterterrorist driving, surveillance detection, and improvised explosive device handling.

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

**1 FAM 262.5-2(A)(1) Overseas Training Branch
(DS/SLTD/OTB)**

(CT:ORG-344; 08-29-2014)

The Overseas Training Branch (DS/SLTD/OTB):

- (1) Develops courses and provides instruction and course coordination for:
 - (a) Basic Regional Security Officer training;
 - (b) Regional Security Officer In-Service training; and
 - (c) Security for Non-Traditional Operating Environments;
- (2) Provides subject-matter expertise for the Foreign Affairs Counter Threat (FACT) Seminar, Security Overseas Seminar, and for the Serving Abroad for Families and Employees (SAFE) training to include briefings on surveillance detection and explosives recognition; and
- (3) Provides specific security training to COMs, DCMs, principal officers, post security officers, FSNIIs, and Marine security guards (MSGs).

**1 FAM 262.5-2(A)(2) Domestic Training Branch
(DS/SLTD/DTB)**

(CT:ORG-344; 08-29-2014)

The Domestic Training Branch (DS/SLTD/DTB):

- (1) Develops courses and provides instruction and course coordination for:
 - (a) Basic Special Agent training;
 - (b) Special Agent In-Service training; and
 - (c) Mobile Field Office training;
- (2) Develops specialized training courses and provides instruction of these courses to the Bureau of Diplomatic Security (DS) and other personnel to meet DS's global mission requirements; and
- (3) Supports as a partner organization (PO), the Federal Law Enforcement Training Center (FLETC).

**1 FAM 262.5-2(A)(3) Special Skills Training Branch
(DS/SLTD/SSB)**

(CT:ORG-344; 08-29-2014)

The Special Skills Training Branch (DS/SLTD/SSB):

- (1) Develops courses and provides instruction and course coordination for:
 - (a) All standardized DS firearms training and qualification to include the standard DS-issued personal and support weapons, and special

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

weapons as approved by the Special Protective Equipment Review Board (SPERB);

- (b) All standardized DS training in Defensive Tactics and Room Entry Tactics in support of special agents' responsibilities to conduct law enforcement activities and protective security operations;
 - (c) All standardized DS Security Driver Training programs in support of special agents' responsibilities to conduct law enforcement activities and protective security operations;
 - (d) All standardized DS Explosive Countermeasures Training in support of the DS security mission to include courses such as Introduction to Explosives and improvised explosive devices (IEDs), Building and Vehicle Searches, X-ray Interpretation, and Post Blast Investigations, etc.; and
 - (e) High-Threat Operations training; and
- (2) Provides subject-matter expertise to the SPERB and all DS directorates relative to standardized tactics and operations for firearms, defensive tactics, room-entry tactics, security driver tactics, and explosive countermeasures.

1 FAM 262.5-2(B) Security Engineering and Computer Security Training Division (DS/TPS/SECD)

(CT:ORG-344; 08-29-2014)

The Security Engineering and Computer Security Training Division (DS/TPS/SECD):

- (1) Develops training for technical security and information assurance and cyber security topics to include technical surveillance countermeasures, technical security systems, and information system security;
- (2) Presents training and briefings to diverse groups to include chiefs of mission, deputy chiefs of mission, Foreign Service personnel, Civil Service personnel, security specialists, security officers, U.S. Navy Seabees, U.S. Marines, cleared American guards (CAGs), construction surveillance technicians, and others throughout the U.S. Government;
- (3) Manages, coordinates, and administers all fundamental and advanced technical surveillance countermeasures and technical security training programs for:
 - (a) Security engineering officers;
 - (b) Security technical specialists;
 - (c) U.S. Navy Seabees;
 - (d) Construction surveillance technicians;

UNCLASSIFIED (U)

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (e) CAGs; and
- (f) Site security managers;
- (4) Manages, coordinates, and administers information assurance and cyber security training programs in compliance with the Federal Information Security Management Act;
- (5) Serves as the principal technical security training representative of the Department to other Federal agencies and groups; and
- (6) Serves as a Tier II Information System Security Line of Business (ISSLOB) Shared Service Provider (SSP) for Information Assurance (IA) and Cybersecurity Role-Based Training. The Office of Management and Budget and the Department of Homeland Security so designated DS/TPS/SECD's Information Assurance Branch (IAB) in July 2010. ISSLOB identifies common information security needs across the Federal Government and delivers product and service solutions to improve information security program performance, reduce costs, and increase efficiency across the Federal enterprise.

1 FAM 262.5-3 Office of Mobile Security Deployments (DS/T/MSD)

(CT:ORG-344; 08-29-2014)

The Office of Mobile Security Deployments (DS/T/MSD):

- (1) Provides emergency security support to posts abroad during periods of high threat, crisis, or natural disaster;
- (2) Assists DS protective details with tactical support, both domestically and abroad, in high-threat situations; and
- (3) Provides specialized training at Foreign Service posts on a variety of security topics, as directed.

1 FAM 262.6 Deputy Assistant Secretary and Assistant Director for Threat Investigations and Analysis (DS/TIA)

(CT:ORG-344; 08-29-2014)

The Deputy Assistant Secretary and Assistant Director for Threat Investigations and Analysis (DS/TIA):

- (1) Reports directly to the Assistant Secretary for Diplomatic Security on matters of threat intelligence, while maintaining normal reporting through the PDAS for all other routine and administrative matters, and directly supplies threat analysis to all DS components, regional Assistant Secretaries and chiefs of mission in order to disseminate key security-

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

related threat information to appropriate individuals rapidly.

- (2) Directs, coordinates, and conducts analysis of information involving terrorist threats and/or hostile activities directed against all U.S. Government personnel, facilities, and interests abroad under Chief-of-Mission authority;
- (3) Directs, coordinates, and conducts protective intelligence investigations;
- (4) Administers the Department's counterterrorism rewards programs (Rewards for Justice Program) (see 12 FAM 226.3);
- (5) Coordinates foreign-government and private-sector requests for assistance relating to terrorist and terrorist-related incidents; and
- (6) Directs, coordinates, and oversees the operations of the DS Command Center and the Overseas Security Advisory Council (OSAC).

**1 FAM 262.6-1 Office of Intelligence and Threat Analysis
(DS/TIA/ITA)**

(CT:ORG-344; 08-29-2014)

The Office of Intelligence and Threat Analysis (DS/TIA/ITA):

- (1) Acts as the interface between DS and the U.S. Intelligence Community on protective intelligence and threat issues to ensure that timely intelligence information is available to DS decision makers, as well as initiates and issues threat notifications to the field;
- (2) Researches, monitors, and analyzes all-source intelligence on terrorist activities and threats directed toward U.S. citizens and U.S. diplomatic and consular facilities abroad, as well as threats against the Secretary of State, senior U.S. officials, visiting foreign dignitaries, resident foreign diplomats, and foreign missions in the United States for which DS has protective security responsibility;
- (3) Provides real-time threat assessments, supporting senior DS and Department officials in policy and operational issues; and
- (4) Prepares the Department's Security Environment Threat List (SETL).

**1 FAM 262.6-2 Office of Protective Intelligence Investigations
(DS/TIA/PII)**

(CT:ORG-344; 08-29-2014)

The Office of Protective Intelligence Investigations (DS/TIA/PII):

- (1) Directs, coordinates, and conducts investigations of external threats as they relate to terrorism, political violence, and suspicious activity directed against the Secretary of State, Department personnel and facilities;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

designated foreign dignitaries and diplomatic facilities in the United States; and all U.S. Government personnel, facilities, and interests under Chief of Mission authority abroad;

- (2) Directs, coordinates, and conducts threat management investigations and directed operations including individual threat assessments, tactical intelligence liaison support, high-risk protection detail enhancement, regional security officer (RSO) incident and program assistance, and protective security (PRS) training augmentation, to assure the safety and security of DS-designated personnel and facilities;
- (3) Provides oversight and direction to DS interagency participation in the Federal Bureau of Investigation (FBI) managed Joint Terrorism Task Force (JTTF), the National Counter Terrorism Center (NCTC), and the Department of Defense Joint Interagency Task Force Program (DoD/JIATF); and
- (4) Administers the Department's Rewards for Justice Program (see 12 FAM 226.3.)

1 FAM 262.6-2(A) Operations and Investigations Division (TIA/PII/OI)

(CT:ORG-344; 08-29-2014)

Through threat management investigations and directed operations to advance the safety and security of DS-designated personnel and facilities, the Operations and Investigations Division (DS/TIA/PII/OI):

- (1) Investigates external threats involving terrorism, political violence, potentially hostile or suspicious activity, operational psychologist threat assessments, and protective intelligence derived from the Intelligence Community;
- (2) Identifies and mitigates threats to DS protection details, special events, and facilities in close collaboration with DS/DO. Protection support can include tactical intelligence liaison, threat analysis and social media monitoring, threat vulnerability identification and assessment, plain clothes /low-profile operations, threat/suspicious activity investigations, inter-agency liaison, and comprehensive analytical support;
- (3) Mitigates threats and provides consultation support to overseas posts in close collaboration with DS/IP, DS/HTP, and RSOs overseas. Overseas assistance can include suspicious activity/specific incident investigations, surveillance detection/plainclothes operations, threat vulnerability assessments, threat awareness and personal safety training, tactical intelligence consultations, and social media monitoring integration; and
- (4) Conducts threat recognition training and verification in close collaboration with DS/T and DS/DO. This support includes protective intelligence support to basic agent classroom and field exercise training, as well as

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

formal after action reviews, lessons learned, and best practices related to support of Secretary's Detail and Dignitary Protection operations.

1 FAM 262.6-2(B) Intelligence Liaison Division (TIA/PII/IL)

(CT:ORG-344; 08-29-2014)

The Intelligence Liaison Division (DS/TIA/PII/IL):

- (1) Manages DS support to the counterterrorism law enforcement community; and
- (2) Coordinates DS participation in terrorism investigations and other activities through the FBI Liaison Program, which is comprised of the JTTF, National Joint Terrorism Task Force (NJTTF), the National Counterterrorism Center (NCTC), and the Department of Defense's (DoD) Joint Interagency Task Force – National Capital Region (JIATF-NCR):
 - (a) The TIA/PII/IL JTTF mission is a collaborative effort with state, local, tribal and Federal law enforcement organizations investigating individuals and organizations planning or committing terrorist acts in violation of Federal statutes applicable to national security efforts in the United States and overseas;
 - (b) The PII/IL NJTTF mission is a strategic-level information-sharing and management effort involving all currently established JTTFs in the U.S., specifically focused on those JTTFs where DS does not have an agent presence. At the national level, NJTTF coordinates DS and Department operational counterterrorism efforts with the FBI and broader interagency;
 - (c) The PII/IL NCTC Liaison Program provides the NCTC with a DS service-link representative, coordinated through INR per 1 FAM 431.1(1) and (5), whose mission is to share and disseminate intelligence information affecting Department interests with the broader United States Government (USG) counterterrorism community; provide crisis management support and response planning for overseas issues affecting the USG; and, support NCTC exercises and special-events to include international and domestic special events; and
 - (d) The PII/IL JIATF-NCR program provides the DoD JIATF-NCR with a DS service-link representative whose mission is to share and disseminate intelligence information affecting Department interests with the DoD. Additionally, the JIATF-NCR program facilitates the exchange of information and coordinates operational efforts with the DoD on matters related to the RFJ program.

1 FAM 262.6-2(C) The Rewards for Justice Program (DS/PII/RFJ)

(CT:ORG-344; 08-29-2014)

The Rewards for Justice Program (DS/TIA/PII/RFJ) is the Department's counterterrorism rewards program. Under RFJ, rewards can be offered and paid for information that:

- (1) Prevents or favorably resolves acts of international terrorism against U.S. persons or property;
- (2) Leads to the arrest or prosecution of individuals responsible for such acts or the location of a key terrorist leader; or
- (3) Disrupts terrorism financing.

1 FAM 262.6-3 Diplomatic Security Command Center (DS/TIA/CC)

(CT:ORG-344; 08-29-2014)

The Diplomatic Security Command Center (DS/TIA/CC) provides the following 24/7 services:

- (1) Manages and collates incoming security-related information regarding threats, security incidents, and unfolding emergency situations and disseminates that information appropriately and rapidly to DS and Department leadership;
- (2) Coordinates threat and security-related information with the Department's Operations Center;
- (3) Disseminates guidance and important information to the field from DS leadership;
- (4) Serves as support and point of contact (POC) for all after-hours calls for DS field offices, RSOs, engineering security centers and offices (ESCs/ESOs), and diplomatic courier divisions;
- (5) Monitors after-hours police liaison issues for DS, to include law enforcement response to incidents involving foreign dignitaries and resident foreign diplomats;
- (6) Monitors the Personnel Tracking Locator (PTL) system—the GPS-based 911 tracking and call-for-help system used by high- and critical-threat protective details—and makes appropriate rapid notifications when an activation occurs;
- (7) Serves as the main point of contact for all DS protective security details, to include monitoring of radio frequencies;
- (8) Serves as DS's after-hours point of contact for the interagency regarding

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

emerging threats and significant events;

- (9) Performs urgent Treasury Enforcement Communications System (TECS) and National Crime Information Center (NCIC) queries for RSOs and special agents in the field, and maintains all DS warrant information;
- (10) Produces the DS Overnight Update, and coordinates and disseminates all spot reports;
- (11) Establishes DS-specific task forces at the discretion of DS leadership;
- (12) Coordinates DS's participation in daily interagency secure-voice teleconferencing;
- (13) Assembles information regarding security incidents, threats, and surveillance activity from abroad and publishes the Diplomatic Security Daily, which is disseminated throughout the security and Intelligence Community;
- (14) Monitors remotely, through the Technical Operations Group (TOG) via the Security Management System enterprise (SMSe) network, selected technical security systems at posts abroad. DS/TIA/CC provides appropriate notification within DS and to the affected post if an event is detected;
- (15) Provides embedded DS/TIA/CC watch officers to the Department Operations Center, the White House Situation Room, and the Department of Homeland Security's (DHS) Operations Center to coordinate the sharing of information; and.
- (16) Provides a command and control infrastructure for DS senior leadership to utilize during times of crises.

1 FAM 262.6-4 Overseas Security Advisory Council

(CT:ORG-344; 08-29-2014)

The Overseas Security Advisory Council (OSAC):

- (1) Is a Federal advisory committee under the auspices of the Secretary of State. Its staff director is resident in DS;
- (2) Establishes continuing liaison and provides for operational security cooperation between the Department security functions and the private sector, which includes U.S. businesses, non-governmental organizations (NGOs), faith-based groups, and academia;
- (3) Provides for regular and timely interchange of information between the U.S. private sector and the Department concerning developments in the security environment abroad;
- (4) Recommends methods and provides material for coordinating security planning and implementation of security programs; and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (5) Recommends methods to protect the competitiveness of U.S. businesses operating worldwide.

1 FAM 262.7 Senior Coordinator for Security Infrastructure (DS/SI)

(CT:ORG-344; 08-29-2014)

The Senior Coordinator for Security Infrastructure (DS/SI) advises the Principal Deputy Assistant Secretary and Director of the Diplomatic Security Service and:

- (1) Manages matters relating to security infrastructure in DS functional areas of information security, computer security, personnel security and suitability, and insider threat;
- (2) Formulates, consolidates, and recommends to the Assistant Secretary strategic operational planning, priorities, and funding for DS security infrastructure operations; and
- (3) Chairs and/or serves on Departmental and/or interagency groups and committees relating to security infrastructure.

1 FAM 262.7-1 Office of Information Security (DS/SI/IS)

(CT:ORG-344; 08-29-2014)

The Office of Information Security (DS/SI/IS):

- (1) Is responsible for the Department's information protection programs as described in this section and sections for the Program Applications Division, Industrial Security Division, and Special Security Operations Division, (see 1 FAM 262.7-1(A), 1 FAM 262.7-1(B), and 1 FAM 262.7-1(C));
- (2) Coordinates certification and accreditation actions on behalf of the Head of Intelligence Community Element (HoICE) as specified in the DS-INR memorandum of agreement (MOA), for all Sensitive Compartmented Information (SCI) systems within a Department facility, domestically, or diplomatic facility abroad;
- (3) Coordinates, implements, and oversees SCI systems policy and procedures and serves as the HoICE, designated accrediting authority (DAA) for SCI systems. DS/SI/IS serves as the HoICE representative to security-related Intelligence Community boards and working groups;
- (4) Participates in damage assessments when Department information has been subjected to compromise and provides investigative and/or prosecutorial support in cases involving unauthorized disclosure or espionage involving Department information or employees. DS/SI/IS plays a role on interagency damage assessment teams;
- (5) Serves as the DS Critical Infrastructure Protection (CIP) coordinator and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

represents DS in Department and other agency forums and facilitates interagency CIP security discussions and sharing of best practices.

DS/SI/IS serves as the primary DS interface with the Bureau of Budget and Planning (BP), which is the Department's CIP program office;

- (6) Enables the secure, appropriate, and effective reciprocal sharing of non-intelligence information critical to the security of the United States with allied governments and international organizations, consistent with Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), and with the establishment of the Information Sharing Environment (ISE);
- (7) Represents DS in intra-Department meetings, and State on some interagency groups that deal with a broad range of national security policy issues, including preparation of directives on how classified national security information and unclassified sensitive information is used to counter 21st century threats;
- (8) In support of the lead bureaus and offices designated by the Secretary, DS/SI/IS engages in allied collaboration and international cooperation with foreign governments and international organizations on priorities such as CISR, cyber security and information sharing;
- (9) Coordinates certification and accreditation actions for Sensitive Compartmented Information facilities (SCIFs) located in diplomatic facilities abroad, including Department and tenant facilities;
- (10) Implements and maintains monitoring center facilities for Department-owned SCI networks' intrusion-detection system (IDS). DS/SI/IS reports SCI system intrusions and incidents to the SCI system owner and oversees remediation;
- (11) Informs the Department HoICE, the Assistant Secretary for Intelligence and Research (INR), and seeks clearance/approval for requisite actions in accordance with applicable Intelligence Community policies and the DS-INR Memorandum of Agreement to certify and accredit Department SCI systems and perform continuous monitoring in accordance with the Federal Information Security Management Act (FISMA);
- (12) Conducts insider threat monitoring on Department SCI systems in coordination with the Bureau of Intelligence and Research (INR);
- (13) Conducts security systems visits of embassy locations requesting SCI video teleconferencing, and, after risks are addressed and minimized, recommends approval of the facility for SCI video conferencing;
- (14) Conducts comprehensive security-vulnerability assessments abroad to determine posts' information and operations security (OPSEC) postures. DS/SI/IS assists regional and post security officers in establishing effective incident prevention, education and awareness, and strong operations security programs;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (15) Develops, implements, and oversees non-Intelligence Community (IC) special access program (SAP) security requirements, to include physical, technical, personnel, automated information system (AIS), telecommunications, operations, and procedures;
- (16) Coordinates Secretary of State approvals of Department-created SAPs and oversees their annual recertification;
- (17) Verifies that SAP participants protect classified information and is responsible for completing SAP systems certification and accreditation (C&A);
- (18) Establishes and oversees foreign exchange officer security requirements for the Transatlantic Diplomatic Fellowship program, and monitors the foreign exchange officer local area networks (LANs). DS/SI/IS ensures that foreign exchange officers meet all security requirements and works with IRM/IA to ensure C&A on these LANs; and
- (19) Addresses major security incidents, such as espionage and other intelligence failures, by coordinating damage assessments for the Department. DS/SI/IS reports these incidents to the IC and elements of the Justice Department to perform national-level damage assessments. DS/SI/IS represents the Department as required, including providing direct support to national counterintelligence executive (NCIX) interagency damage assessment teams.

1 FAM 262.7-1(A) Program Applications Division (DS/IS/APD)

(CT:ORG-344; 08-29-2014)

The Program Applications Division (DS/IS/APD):

- (1) Administers the Department's information protection program, as described in this section;
- (2) Develops, implements, and oversees policies and procedures for the safeguarding of national security information in accordance with national laws, orders, and directives, and consults with agency members of the national security community to aid in the exchange of internal agency policies and directives;
- (3) Develops, implements, and oversees policies and procedures for the safeguarding of administratively controlled information designated as Sensitive But Unclassified (SBU);
- (4) Provides procedural and operations security direction, guidance, and assistance to all bureaus and posts utilizing e-mail help desks, on-site reviews, security notices, and other available means;
- (5) Manages an information security education, training, and awareness program, and provides initial indoctrination and refresher briefings;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (6) Administers the Department's Cyber Security Incident Program (CSIP) to ensure the integrity, confidentiality, and availability of sensitive Department IT systems through thorough investigations of potential cyber-security incidents to protect the Department cyber infrastructure from potential damage or risk (see 12 FAM 590);
- (7) Administers the Department's Security Incident Program and coordinates cases subject to disciplinary action with the Bureau of Human Resources, Employee Relations Division (HR/ER), personnel security clearance actions DS, and SCI access actions with INR, and DS. Conducts incident investigations to include those involving communications security (COMSEC) that initially indicate the possible compromise of classified information, and SCI;
- (8) Manages the Department's domestic Bureau Security Officer Program and Unit Security Officer Program; designed to implement effective internal security controls throughout the Department;
- (9) Develops, implements, and oversees a Department OPSEC program in accordance with national directives, conducts OPSEC surveys, and provides OPSEC program training;
- (10) Coordinates investigations with DS and other agency investigative elements as required;
- (11) Develops, implements, and oversees the requirements for classified information open storage; approves all open-storage areas/facilities, and administers a recertification program;
- (12) Ensures that standards have been met before granting requests for classified conference room approvals and oversees secure video teleconferencing; and
- (13) Represents DS in intra-Department meetings and State on interagency groups that deal with OPSEC and other information security issues.

1 FAM 262.7-1(B) Industrial Security Division (DS/IS/IND)

(CT:ORG-344; 08-29-2014)

The Industrial Security Division (DS/IS/IND):

- (1) Manages the Department's implementation of the National Industrial Security Program (NISP) and administration to ensure the proper handling of classified and SBU information and assets entrusted to or generated by private industry;
- (2) Develops, implements, and oversees policies, standards, and procedures for the protection of classified information and specifically designated unclassified information provided to Department contractors and consultants;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (3) Analyzes procurement documentation and ensures that appropriate security requirements are incorporated into all contracts in support of the Department's classified and specified SBU acquisitions;
- (4) Develops policies and ensures the implementation of procedures for the disclosure of national security and other sensitive information to firms with significant foreign ownership, control, or influence;
- (5) Develops, implements, and administers an industrial security compliance program and conducts inspections of Department contractors to ensure their adherence to Department and national industrial security requirements;
- (6) Serves as the Department's liaison with NISP managers and serves as the Department's primary liaison with the Department of Defense and other Federal agencies in administering an effective industrial security program;
- (7) Reviews and approves visit authorizations for cleared-contractor personnel, ensuring their access is consistent with contract-security requirements;
- (8) Assists and assures the quality and expeditious processing of contractor-personnel security clearances and public-trust determinations the Department conducts for high-priority contracts;
- (9) Conducts industrial security program briefings for contracting officers, contracting officers' representatives, and program managers. DS/IS/IND provides industrial security briefings and other educational materials to contractor facilities and employees;
- (10) Coordinates the security review and analysis of proposed foreign acquisitions of U.S. firms and provides the consensus DS position to the Bureau of Economic Business Affairs (EB) in support of the Committee on Foreign Investment in the United States (CFIUS);
- (11) Coordinates system connectivity requirements of contractors connecting to Department information systems and oversees compliance. DS/IS/IND ensures requirements are established in conjunction with 1 FAM 271.2 e(6)(a);
- (12) Ensures the incorporation of the appropriate security requirements into all contracts in support of the Department's Overseas Buildings Operations (OBO) classified and SBU acquisitions, provides full-time industrial security support to OBO, provides ongoing training to OBO contractors and OBO personnel, as well as regional security officers/site security managers, and coordinates resolution of contractor's violations of security requirements specified in OBO contracts;
- (13) Acts as a liaison with the Defense Security Service to obtain facility clearances for uncleared firms requiring access to classified information, either during the bid phase or for contract performance, and resolves issues arising during the processing of the firms for facility clearances;

UNCLASSIFIED (U)

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (14) Ensures that SCI security requirements are included in specific classified contracts, and processes requests for SCI access for contractor personnel assigned to such contracts; and
- (15) Represents DS in intra-Department meetings and State on interagency groups that deal with industrial-security issues.

**1 FAM 262.7-1(C) Special Security Operations Division
(DS/IS/SSO)**

(CT:ORG-344; 08-29-2014)

The Special Security Operations Division (DS/IS/SSO):

- (1) Coordinates and implements policies and procedures to ensure that intelligence information, including SCI, is disseminated and used securely in accordance with applicable Intelligence Community policies including: Intelligence Community Directives (ICDs), Intelligence Community Policy Guidance (ICPGs), Intelligence Policy Memorandums (ICPMs), Intelligence Community Standards (ICSs) and Director of Central Intelligence Directives (DCIDs);
- (2) Establishes and maintains a secure document control system for SCI materials and provides for the accountability and control of designated SCI documents. DS/IS/SSO conducts a continuous review of designated SCI document flow into, within, and out of the Department and ensures the timely and secure dissemination of designated SCI intelligence to Department decision makers;
- (3) Performs the document control function for all issues involving the SCI Human Intelligence (HUMINT) Control System (HCS) subcompartments and maintains full control of the only accredited repository for storage of these sensitive documents. DS/IS/SSO conducts indoctrination briefings for the HCS subcompartments before individuals are granted access and debriefing when individuals no longer require access;
- (4) Responds to HCS queries regarding the handling, processing, distribution, or destruction of HCS documents and notifies the Central Intelligence Agency (CIA) HCS Program Office of any HCS mishandling incidents, and ensures corrective measures are enforced;
- (5) Manages the IntelTRUST program at State, including processing requests for access, conducting inspections of facilities/offices designated for IntelTRUST access, and conducting briefings/debriefings;
- (6) Coordinates implementing policies and procedures to protect SCI and SCI-indoctrinated personnel from intelligence or counterintelligence (CI) threats as a consequence of hazardous travel, in accordance with applicable Intelligence Community policies;
- (7) Provides SCI security education and awareness for Department personnel

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

by means of the SSO Web site, the issuance of Department Notices, SCI access indoctrinations, and debriefings;

- (8) Coordinates, implements, and oversees policies, plans, and procedures for the certification and accreditation of SCIFs in accordance with applicable Intelligence Community policies. DS/IS/SSO serves as the cognizant security authority (CSA) for Department SCIF accreditation and operations both domestically and abroad and coordinates SCIF certification with the Office of the Director of National Intelligence (ODNI) officials;
- (9) Ensures that technical surveillance countermeasures (TSCMs) are conducted in all Department SCIFs in accordance with applicable Intelligence Community policies;
- (10) Manages SCI security policies and access control procedures for all Department SCIFs and conducts SCIF periodic security reviews (PSRs);
- (11) Reviews and approves physical security preconstruction plans for Department SCIF construction, expansion, or modification;
- (12) Monitors all Department SCIF construction, expansion, or modification to ensure that the integrity of the facility is properly maintained;
- (13) Evaluates the threat to Department SCIFs and coordinates policies and standards to protect SCI material;
- (14) Provides updates to the ODNI SCIF database on all Department SCIFs;
- (15) Processes all SCI nominations for all Department employees, contractors, and detailees for access to SCI. DS/IS/SSO coordinates all Department-related requests for SCI access with the Head of Intelligence Community Element (HoICE) Determination Authority (DA), and DS's Office of Personnel Security and Suitability (DS/SI/PSS). DS/IS/SSO maintains a database of all Department personnel with SCI access;
- (16) Serves as the office of primary responsibility for the passing of SCI accesses through proper channels;
- (17) Informs the Department HoICE, the Assistant Secretary for Intelligence and Research (INR), and seeks clearance/approval for requisite actions in accordance with applicable Intelligence Community policies and the DS-INR (MOA); and
- (18) Represents DS in intra-Department meetings and State on interagency groups that deal with SCIF standards and access.

1 FAM 262.7-2 Office of Computer Security (DS/SI/CS)

(CT:ORG-344; 08-29-2014)

The Office of Computer Security (DS/SI/CS):

- (1) Recommends, develops, and coordinates cyber security policy, standards,

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

and guidelines;

- (2) Recommends, develops, and coordinates all waivers and exceptions to Department cyber security policy;
- (3) Assesses emerging cyber security technology and provides findings to senior management, including the Chief Information Officer (CIO), the Assistant Secretary for Diplomatic Security, Chief Information Security Officer (CISO), Deputy CIO for Operations, and system owners;
- (4) Oversees and manages the Evaluation and Verification Program;
- (5) Provides technical expertise to support the Department's information security (INFOSEC) program as it relates to the protection of collateral information;
- (6) Conducts computer security assessments (CSAs) of Department sites and systems;
- (7) Conducts detailed security and safeguards analyses of software and firmware used in the Department's information technology (IT) systems;
- (8) Updates and documents computer security program development and changes to support the Senior Coordinator for Security Infrastructure (DS/SI);
- (9) Identifies and implements cyber security technology to support the Department's technical counterterrorism and CI capabilities;
- (10) Manages the Overseas Security Policy Board (OSPB) Information Systems Security Working Group (ISSWG) for the development of uniform computer security standards for all foreign affairs agencies serving under chief-of-mission authority;
- (11) Approves cyber security-related waivers and exceptions to OSPB standards and coordinates, in conjunction with IRM, waivers and exceptions to OSPB standards for Department elements;
- (12) Represents the Department as the primary representative for the Committee on National Security Systems (CNSS), Department of Homeland Security (on cyber security issues), and United States Computer Emergency Readiness Team (for cyber incident reporting);
- (13) DS/IS/CS has direct liaison work with National Cyber Investigative Joint Task Force (NCIJTF), NSA National Threat Operations Center (NTOC), U.S. Computer Emergency Readiness Team (US-CERT), USCYBERCOM, and other U.S. government elements on operational security matters affecting the Department's personnel, information, and IT assets;
- (14) Creates and delivers the cyber security awareness program for all Department users, including system administrators, information systems security officers (ISSOs), and managers and chief executives, briefing them on IT security responsibilities, risks to information and systems; and

UNCLASSIFIED (U)

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

related policies and controls to mitigate those risks, as approved by the Chief Information Security Officer (CISO);

- (15) Approves the unattended operation of IT systems that process classified information at CRITICAL THREAT posts;
- (16) Directs, manages, and maintains the Department's overall capacity for network intrusion detection, monitoring, incident handling and response, and cyber threat analysis relating to the Department's secret collateral and below systems. DS/SI/CS provides technical analysis and assistance to DS and other Federal law enforcement agencies; for TS/SCI networks see 1 FAM 262.7-1 (10);
- (17) Manages a cadre of U.S. Government IT security specialists to act as regional computer security officers (RCSOs) to provide on-site customer support, training, and oversight to Department employees worldwide;
- (18) Researches, develops, and maintains security configuration standards and guidelines for Departmental implementation of IT hardware and applications. DS/SI/CS provides ongoing assistance to Department system managers, applications developers, and Department- and bureau-level configuration control boards to ensure IT security requirements are included in life-cycle management of systems and applications;
- (19) Develops and maintains a cyber threat analysis and reporting capability to support Department-level threat determinations and subsequent vulnerability mitigation;
- (20) Coordinates on cyber threats to the Department with the Intelligence Community, Department of Homeland Security, and other U.S. government elements;
- (21) Conducts continuous and directed network- or application-specific vulnerability assessment testing, independent penetration testing, and intelligence monitoring to identify specific risks to those systems and develops risk mitigation strategies to protect the Department's IT infrastructure;
- (22) Develops, in conjunction with the Bureau of Information Resource Management's Office of the Deputy Chief Information Officer for Operations, (IRM/OPS), cyber security procedures for operational elements;
- (23) Conducts security analyses, independent vulnerability assessments, and selective cyber security control reviews of IT systems;
- (24) Provides oversight for the overall monitoring of Department telecommunications resources, systems, and networks, to include detection and response to security-related incidents involving telephones or telephone equipment;
- (25) Provides for the development and use of automated validation tools to

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

perform compliance monitoring and reporting; and

- (26) Maintains and operates, in coordination with IRM, key components of the Department's Situational Awareness Program, to include input from continuous scanning, advanced threat monitoring and analysis, site scoring, and RSCOs; and
- (27) Works to ensure compliance with the Department's information security program requirements in coordination with CIO, CISO, and IRM/OPS.

1 FAM 262.7-2(A) Monitoring and Incident Response Division (DS/CS/MIR)

(CT:ORG-344; 08-29-2014)

The Monitoring and Incident Response Division (DS/CS/MIR):

- (1) Maintains a comprehensive layered intrusion-detection system (IDS) program to proactively monitor and audit information systems; detect inappropriate, malicious, or anomalous activity; and issue warnings and alerts for possible unauthorized access. DS/CS/MIR provides real-time situational awareness for the Department's networks and information systems worldwide;
- (2) Maintains a Computer Incident Response Team (CIRT) to serve as the Department's focal point for reporting computer and cyber security incidents impacting Department and foreign affairs agencies' networks (i.e., information about incidents is shared and coordinated with operational managers, law enforcement within the Bureau of Diplomatic Security (DS), and outside agencies as appropriate, to support criminal prosecution) 24 hours a day, 7 days a week, 365 days a year (24x7x365);
- (3) Reports incident information to the U.S. Computer Emergency Readiness Team (US-CERT) and participates in the quarterly US-CERT partners meetings where Federal incident response teams, law enforcement, private-sector representatives, and academics exchange ideas and examine technical issues. DS/CS/MIR acts as liaison with other Federal and Department of Defense (DOD) CERTs for the exchange of information and reporting of computer security incidents;
- (4) Determines computer misuse and provides remediation procedures and technical assistance for criminal investigations;
- (5) Provides and maintains the capability for the overall monitoring of Department telecommunications resources, systems, and networks, to include detection and response to security-related incidents involving telephones or telephone equipment, and refers telephone security incidents to the DS investigative authority;
- (6) Supports the Department's defense in-depth strategy by maintaining systems to monitor network and host information systems for

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

vulnerabilities and configuration compliance status, as well as inappropriate, incorrect, malicious, unauthorized, or anomalous activity. These systems include:

- (a) A host-vulnerability scanning system;
 - (b) A configuration-compliance scanning system; and
 - (c) Application-vulnerability assessment software, such as Web-application security tools and database-security scanners;
- (7) Conducts continuous monitoring for vulnerabilities and configuration compliance of hardware and software used in the Department's computer and communications sites that process classified, unclassified, and SBU information, and provides that information for inclusion in the Department's Risk Scoring Program; and
- (8) Provides for the development and use of automated validation tools to perform compliance monitoring and reporting.

1 FAM 262.7-2(B) Cyber Threat Analysis Division (DS/CS/CTA)

(CT:ORG-344; 08-29-2014)

The Cyber Threat Analysis Division (DS/CS/CTA):

- (1) Maintains an in-depth cyber threat analysis capability to provide posts abroad and senior Department management with indications and warnings via extensive analysis as well as daily and specialized reporting of cyber threats impacting the Department's critical infrastructure;
- (2) Consolidates and analyzes information and data from the firewall team, Network Monitoring Center, Computer Incident Response Team (CIRT), Intelligence Community, and U.S. Government agencies to produce a comprehensive, all-source threat picture of the Department's critical infrastructure;
- (3) Serves as the Department's "information broker" for cyber threat information by routinely disseminating cyber threat information to upper management, RSOs, RCSOs, information security officers (ISOs), Virus Incident Response Team, CIRT, Network Monitoring Center, DS/ICI/CI, DS/ICI/CR, and firewall team;
- (4) Helps satisfy Federal information-sharing requirements through active liaison with the Computer Network Defense Law Enforcement and Intelligence communities of interest that have significant cyber security responsibilities, including relationships with the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), National Security Agency (NSA)-National Threat Operations Center, National Cyber Investigative Joint Task Force, Office of the National Counterintelligence Executive U.S. Strategic Command, Defense Intelligence Agency (DIA),

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1

Organization and Functions

Central Intelligence Agency (CIA), and the DoD Joint Task Force-Global Network Operations (JTF-GNO);

- (5) Produces comprehensive cyber threat assessments and analysis regarding State and non-State entities that may pose a threat to the Department's IT infrastructure for the Department's systems and management staff;
- (6) Assists in determining the threat posed to the Department's critical IT infrastructure and functions as the Department's all-source fusion cell by merging cyber threat information and analysis;
- (7) Produces cyber threat advisories, special reports, and comprehensive threat assessments concerning threats to, and potential vulnerabilities of, Department networks;
- (8) Conducts independent penetration tests and threat assessments related to vulnerabilities associated with the Department's IT systems and provides cyber threat analysis information for use in the Department's Risk Scoring Program;
- (9) Identifies vulnerabilities through a combination of assessments and testing of the Department's network resources, including full-scope red teaming, penetration testing, and advanced analyses addressing system assets; potential undesirable cyber events; the motives, intentions, capabilities, and history of adversaries; exploiting security weaknesses; risks; and the costs and impacts of countermeasures to ensure integrity of the Department's architecture;
- (10) Conducts advanced analyses and trends analysis of malicious activity against the Department's critical infrastructure;
- (11) Conducts malware analysis and network intrusion forensics on Department hardware drives and mobile computing devices;
- (12) Provides technical and analytical support to DS/ICI/CI; and
- (13) Maintains and operates the DS advanced threat monitoring and analysis capability.

1 FAM 262.7-2(C) Enterprise Technology, Policy and Awareness Division (DS/CS/ETPA)

(CT:ORG-344; 08-29-2014)

The Enterprise Technology, Policy and Awareness Division (DS/CS/ETPA):

- (1) Recommends, develops, and coordinates certain clearances of Department computer, communications, and network security policies, standards, and guidelines. This policy-related activity covers computer/network security (COMPUSEC) policy and standards that define the Department's minimum security requirements for automated information systems (AISs), AIS networks (local area networks (LANs)), and worldwide area networks

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

(WANs), as well as communications security (COMSEC) policy that stipulates security requirements for the environment and equipment;

- (2) Serves as the Co-Chair of the Cyber Security Policy Development Working Group (CSPDWG) that coordinates the development of 12 FAM 600 and 12 FAH-6 H-540 cyber security policies and procedures;
- (3) Recommends, develops, and coordinates clearance of waivers and exceptions to Department computer, communications, and network security policies;
- (4) Chairs the OSPB ISSWG that is responsible for updating the OSPB security standards in 12 FAH-6 H-540, Automated Information Systems (AISs). The group is comprised of members from all U.S. Government agencies that operate abroad under chief-of-mission authority;
- (5) Manages, recommends, develops, and coordinates all OSPB-related waivers and exceptions to classified and unclassified computer security standards;
- (6) Recommends and coordinates the approval of domestic, unattended operations of Department IT systems that process classified information;
- (7) Recommends and coordinates the approval of unattended operations of Department IT systems that process classified information at CRITICAL-THREAT posts;
- (8) Reviews, coordinates, and develops the Department's position on national-level classified computer and communications security policies and INFOSEC voted upon by the Department's Committee on National Security Systems (CNSS) representative, the Senior Coordinator for Security Infrastructure;
- (9) Serves as the Co-Chair of the Awareness, Training, Education, and Professionalism (ATEP) Working Group that oversees the planning and content of all Department security awareness training, role-based training, education, and professional programs;
- (10) Through the Cyber Security Awareness Program, provides timely and accurate guidance to all Department users ensuring all personnel are aware of current policies and procedures as well as their role and accountability in reducing information security risks associated with their activities. DS/CS/ETPA initiates, develops, disseminates, and provides computer security awareness training to all Department IT users, managers, and operators. The CISO approves awareness programs; and
- (11) Coordinates and develops Web-based cyber security awareness training targeting users on Department unclassified and classified systems; disseminates current and new standards and policies; and develops Department notices and worldwide messages on issues of immediate concern to the Department community. The CISO approves training curricula.

1 FAM 262.7-2(D) Evaluation and Verification Program

(CT:ORG-344; 08-29-2014)

The Evaluation and Verification Program provides technical expertise in support of the Department's INFOSEC program, including developing the technical rationale for changes in INFOSEC policy, and also provides specialized technical training to DS personnel, as needed. In addition, the program conducts product testing to ascertain security requirements prior to implementation on Department systems or applications by researching, developing, and maintaining security configuration standards and guidelines for Departmental implementation of IT hardware and applications. The program also performs other duties as assigned.

1 FAM 262.7-3 Office of Personnel Security and Suitability (DS/SI/PSS)

(CT:ORG-344; 08-29-2014)

The Office of Personnel Security and Suitability (DS/SI/PSS):

- (1) Is responsible for the Department's Personnel Security and Suitability Programs;
- (2) Administers the contract background security investigator program, comprised of over 1,000 investigators worldwide; and
- (3) Develops, implements, and oversees the Department's policy on personnel security investigations and their subsequent adjudication.

1 FAM 262.7-3(A) Investigations and Adjudications Divisions 1 and 2 (DS/PSS/IA1 and DS/PSS/IA2)

(CT:ORG-344; 08-29-2014)

The Investigations and Adjudications Divisions 1 and 2 (DS/PSS/IA1 and DS/PSS/IA2):

- (1) Conduct personnel security and/or suitability investigations of employees, applicants, contractors, and others seeking access to Department information and/or facilities;
- (2) Direct the conduct of such investigations abroad for other Federal agencies;
- (3) Conduct file reviews on behalf of the HoICE, in accordance with Intelligence Community Directive 704 and its associated policy guidance, and recommending eligibility for Sensitive Compartmented Information (SCI) access to the HoICE Determination Authority; and
- (4) Make security clearances eligibility determinations and public trust certifications for current employees, applicants for employment, certain contractor personnel in support of the critical mission, and others seeking

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

access to Department information and facilities.

1 FAM 262.7-3(B) Adverse Actions (DS/PSS/AA)

(CT:ORG-344; 08-29-2014)

Adverse Actions (DS/PSS/AA):

- (1) Serves as single point of contact for DS for all requests for investigative records checks, e.g., promotion, tenure, Deputy Secretary (D) Committee, etc., to the Bureau of Human Resources (HR);
- (2) Serves on ad-hoc interagency working groups to address personnel security issues throughout the U.S. Government; and
- (3) Determines the suspension, revocation, or subsequent reinstatement of security clearances for personnel, under the cognizance of DS/SI/PSS, as well as performs adjudicative determinations recommending assignment restrictions for Department personnel.

1 FAM 262.7-3(C) Customer Service Division (DS/PSS/CS)

(CT:ORG-344; 08-29-2014)

The Customer Service Division (DS/PSS/CS):

- (1) Assists Department personnel and HR specialists in every aspect of the security clearance process, to include the performance of training requirements;
- (2) Reviews initial security clearance request documentation for consideration of an interim security clearance, upon request, and adjudicates, appropriately and responsibly, for interim access suspension/withdrawal;
- (3) Manages and maintains the personnel security records program;
- (4) Verifies and certifies security clearances on all applicants under reciprocity standards;
- (5) Processes frequent visitors to and from Department facilities and other agencies;
- (6) Administers the Contract Review Panel and security/suitability determinations for contract applicants/employees to the Department; processes and has final determination authority for all reconsideration requests;
- (7) Coordinates all case referrals to the Civil Service Personnel Review Panel and provides DS representation to the panel. The Customer Service Division works with the panel chairperson in establishing case agenda; and
- (8) Is co-responsible with other areas of personnel security and suitability (PSS) for final draft, review, and completion of Presidential-appointee

summary packages.

1 FAM 262.8 Public Affairs (DS/PA)

(CT:ORG-344; 08-29-2014)

The Public Affairs staff (DS/PA), under the direct supervision of the Principal Deputy Assistant Secretary and Director of the Diplomatic Security Service:

- (1) Advises the Assistant Secretary for DS on media relations and outreach efforts;
- (2) Formulates DS press guidance for the Secretary's Spokesperson and responds to all media inquiries regarding DS and security measures at the Department;
- (3) Formulates and conducts an outreach program to inform the public and constituent audiences about DS's activities;
- (4) Coordinates production of all DS media, including managing the DS public Web site; and
- (5) Develops and disseminates materials to the public, the media, and Department personnel on the Department's security programs and DS activities.

1 FAM 263 Executive Director for Diplomatic Security (DS/EX)

(CT:ORG-344; 08-29-2014)

The Executive Director for Diplomatic Security (DS/EX):

- (1) Reports directly to the Assistant Secretary for Diplomatic Security (DS).
- (2) Serves as the principal adviser on management, policy, administrative, planning, and resource issues;
- (3) Provides executive direction and management oversight to:
 - (a) The Deputy Executive Director, who oversees the day-to-day operations of the Directorate;
 - (b) Office of Management Services (DS/EX/MGT);
 - (c) Office of the Chief Financial Officer (DS/EX/CFO);
 - (d) Office of the Chief Technology Officer (DS/EX/CTO); and
 - (e) Human Resources Management (DS/EX/HRM);
- (4) Develops and implements administrative and management policies, plans, and procedures to ensure that DS resources are allocated, administered, and accounted for, in accordance with U.S. law and U.S. Government

regulations;

- (5) Develops and implements the priorities and program objectives of the DS Assistant Secretary, using principles of efficient and cost-effective management and internal controls;
- (6) Provides centralized administrative services, including financial management, contractual and procurement management, personnel management, general services, and automated systems; and
- (7) Provides oversight, in conjunction with the Office of Career Development and Assignments (HR/CDA), to the career development and assignment functions for DS Foreign Service specialist skill code employees.

1 FAM 263.1 Office Management Services (DS/EX/MGT)

(CT:ORG-344; 08-29-2014)

The Office of Management Services (DS/EX/MGT) provides comprehensive management and administrative services to DS, including:

- (1) Administrative, logistics, and general services;
- (2) Contracting and procurement services;
- (3) Policy analysis and planning; and
- (4) Freedom of Information Act (FOIA) and Privacy Act (PA) requests.

1 FAM 263.1(A) Logistics Services Division (DS/MGT/LS)

(CT:ORG-344; 08-29-2014)

The Logistics Services Division (DS/MGT/LS) provides a full range of administrative and logistics services to DS, including:

- (1) DS facilities and space planning, including design, construction oversight, installation, cost estimates, preparation of charters, maintenance, and parking control;
- (2) Property management for DS administrative and program property domestically and abroad;
- (3) Motor vehicle management for the General Services Administration (GSA) and commercial-leased vehicles, including accident reporting, tort claim processing, acquisition, disposal, maintenance, and fleet-card oversight;
- (4) Administration of the Department's travel management program for DS to include travel authorizations, vouchers, training, and control;
- (5) U.S. Government travel card program management for DS;
- (6) Copier management program for DS; and

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (7) Coordination of other DS domestic administrative programs.

1 FAM 263.1(B) Contracting and Procurement Division (DS/MGT/CAP)

(CT:ORG-344; 08-29-2014)

The Contracting and Procurement Division (DS/MGT/CAP) provides a full range of acquisition and procurement services to DS leading to the acquisition of supplies, services and equipment, interagency acquisition agreements (IAAs), personal service contracts (PSCs), credit card purchases, and Federal assistance awards. DS/MGT/CAP:

- (1) Coordinates and processes all DS-initiated procurements including requisitions and small purchases (e.g., credit card, contracts, delivery orders, and blanket purchase orders);
- (2) Develops (and/or assists in the development of) personal service contracts, statements of work, justifications and approvals (J&As) for sole source requirements, and determinations and findings (D&Fs) for claims arising from unauthorized commitments/ratifications and proposals;
- (3) Develops, negotiates, awards, administers, and interprets policy for all DS Federal assistance awards (i.e., grants and cooperative agreements);
- (4) Administers and supplements administration of personal service contracts, interagency acquisition agreements, and resultant military interdepartmental purchase requests (MIPRs), contracts, etc;
- (5) Provides technical advice and guidance to DS program offices in recommending the best procurement/contracting approach;
- (6) Manages DS active contracts, including delivery-order preparation requests; and
- (7) Provides U.S. Government purchase card administration and oversight.

1 FAM 263.1(C) Policy and Planning Division (DS/MGT/PPD)

(CT:ORG-344; 08-29-2014)

a. The Policy and Planning Division (DS/MGT/PPD) is responsible for:

- (1) Developing, clearing, and coordinating policy, including:
 - (a) Coordinating DS changes to the FAM, including clearance, and final approval of Volume 12, Diplomatic Security, and its accompanying FAHs;
 - (b) Providing assistance in policy development to DS program offices and senior managers;
 - (c) Facilitating inter- and intra-agency committees, councils, and working

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

groups; and

- (d) Functioning as the primary liaison with other agencies and organizations, particularly in developing the FAMs/FAHs;
- (2) Developing, maintaining, and evaluating strategic plans and performance measurement systems:
 - (a) Developing and managing the DS operational and strategic planning, program management, and performance measurement programs to integrate policy initiatives, organizational goals, and post and program requirements with resource availability;
 - (b) Preparing the DS annual performance plans and working with the Office of Strategic and Performance Planning to incorporate portions into Department-wide plans and preparing performance reports for the Office of Management and Budget (OMB) and Congress; and
 - (c) Coordinating vulnerability assessments and internal control reviews; evaluating proposed DS corrective actions to ensure they represent an effective and cost-beneficial approach for resolving identified weaknesses or vulnerabilities; and tracking and monitoring the implementation of all corrective actions;
- (3) Responding to legislative and interagency issues; and
- (4) Developing all memoranda of understanding/agreement (MOUs/MOAs) in conjunction with DS program managers and other Department offices and Federal, state, and local government agencies, and maintaining the centralized DS MOUs/MOAs repository.
- b. DS/MGT/PPD coordinates diplomatic security and countermeasures policy issues with all elements of the Department and other foreign affairs agencies.
- c. DS/MGT/PPD serves as the Executive Secretariat for the Overseas Security Policy Board (OSPB) and Special Protective Equipment Review Board (SPERB) and coordinates all activities of the Boards, the various working group standards development activities, and assists in the resolution of difficult issues between agencies. DS/MGT/PPD develops and issues security standards in coordination with the Department and the interagency OSPB.
- d. DS/MGT/PPD oversees DS's compliance with the Office of the Inspector General (OIG), the Government Accountability Office (GAO) audits and inspection recommendations, and Accountability Review Board (ARB) recommendations.
- e. DS/MGT/PPD serves as the Bureau Evaluation Officer and manages evaluation and monitoring for the Bureau.

1 FAM 263.1(D) Freedom of Information and Privacy Acts Division (DS/MGT/FOIA-PA)

(CT:ORG-344; 08-29-2014)

The Freedom of Information and Privacy Acts Division (DS/MGT/FOIA-PA):

- (1) Responds to all inquiries assigned to DS under the Freedom of Information Act (FOIA) (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and applicable Executive Orders (E.O.s) for records or information DS originates. DS/MGT/FOIA-PA responds on behalf of the Bureau to special requests for document production and justifies release or denial decisions in the amendment, appeal, and/or litigation processes;
- (2) Provides policy guidelines to Bureau components on information management as mandated by the Privacy Act, the Freedom of Information Act, and applicable executive branch directives;
- (3) Serves as DS' primary point of contact for customers in matters pertaining to security records life-cycle management, public, and need-to-know access to security information, classification management and declassification, privacy, and research of official security records; and
- (4) Coordinates, as appropriate, with the Office of Information Programs and Services (A/GIS/IPS) and the Office of the Legal Adviser for Management (L/M), which has Department-wide responsibilities for Freedom of Information Act and Privacy Act matters.

1 FAM 263.2 Office of the Chief Financial Officer (DS/EX/CFO)

(CT:ORG-344; 08-29-2014)

The Office of the Chief Financial Officer (DS/EX/CFO):

- (1) Directs all aspects of DS financial resources;
- (2) Acts as the primary liaison between DS and the Department's financial bureaus, including the Bureau of the Comptroller and Global Financial Services (CGFS) and the Bureau of Budget and Planning (BP);
- (3) Participates in the program planning process to facilitate estimation of future resource needs commensurate with policy goals and objectives;
- (4) Develops and implements strategies for effective and persuasive presentation of budget requests for increased funding, as part of the Department's budget submission to OMB, and the President's Budget to Congress;
- (5) Coordinates with and advises DS program managers and senior officials on all budget and financial matters;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (6) Provides direct supervision to all embedded program Resource Managers;
- (7) Prepares the annual financial plan for all DS operating accounts;
- (8) Requests and justifies additional resources for any unforeseen emergent unfunded requirements within the Diplomatic and Consular Program (D&CP) appropriation, as part of the Department's annual financial planning and quarterly review process, or emergency supplemental request to Congress;
- (9) Monitors the execution of approved financial plans and recommends the reprogramming of resource allocations to DS' Resource Board throughout the fiscal year;
- (10) Oversees the transfer of appropriated funds and reimbursements and helps develop and negotiate agreements with other bureaus and other U.S. Government agencies;
- (11) Certifies funding availability for all DS obligations (i.e., travel authorizations, procurement actions, etc.) and provides fiscal data for obligating documents;
- (12) Maintains appropriate management and internal control systems to safeguard all financial resources are against waste, fraud, unauthorized use, or misappropriation; ensures that obligations incurred comply with applicable laws and regulations, and that revenues and expenditures are promptly recorded and accounted for, in accordance with Departmental procedures; and
- (13) Proactively Identifies program areas where potential for waste, fraud, unauthorized use, or misappropriation of financial resources exists, and pursues systematic resolution.

1 FAM 263.2(A) Financial Execution Division (DS/CFO/FE)

(CT:ORG-344; 08-29-2014)

The Financial Execution Division (DS/CFO/FE):

- (1) Ensures that obligations incurred comply with applicable laws and regulations, and that revenue and expenditures are promptly recorded and accounted for, in accordance with Departmental procedures;
- (2) Executes the DS budget that Congress approves:
 - (a) Allotting funds to Foreign Service posts abroad;
 - (b) Certifying funds available for all domestic obligations; and
 - (c) Monitoring the status of worldwide allotments, obligations, and expenditures;
- (3) Creates and maintains auditable files for all valid obligations;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (4) Serves as the primary liaison between DS and the Global Financial Operations Directorate (CGFS/F), Global Financial Management Systems Directorate (CGFS/GFMS), Financial Policy, Reporting and Analysis Directorate (CGFS/FPRA), and the Bureau of Budget and Planning (BP) concerning budget execution matters;
- (5) Provides support on all matters relating to DS' financial management system, including reviewing financial management system changes and enhancements to ensure that proper management and accounting controls are maintained;
- (6) Performs reconciliation of financial data between the Department's Global Financial Management Systems (GFMS) and DS' financial management system;
- (7) Audits domestic financial activity for compliance with DS policy and applicable laws and regulations;
- (8) Identifies, verifies, and reports Anti-Deficiency Act violations and institutes corrective action when feasible;
- (9) Ensures accuracy, quality, and timeliness of the financial data by tracking and preparing financial management information reports on the status of funds by:
 - (a) Appropriation;
 - (b) Allotment;
 - (c) Obligation;
 - (d) Sub-objective; and
 - (e) Performance goal;
- (10) Oversees the interface of DS's accounting system and other Departmental systems;
- (11) Maintains the domestic representational account for the Assistant Secretary, reimbursing senior management as Department guidelines require, for approved representational expenses. DS/CFO/FE reconciles the representational checking account to bank statements and keeps accountable records for all disbursements;
- (12) Monitors and verifies fiscal information for all purchase card accounts;
- (13) Ensures appropriate separation of duties in accordance with regulations and accounting standard operating practices, reviews and revises internal control processes, and streamlines financial management processes;
- (14) Oversees the transfer of appropriated funds and reimbursements, and helps to develop and negotiate agreements with other bureaus and other U.S. Government agencies; and
- (15) Provides data documentation and other support regarding reimbursable

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

earnings to accommodate accounts receivable, to ensure collection of earned income.

1 FAM 263.2(B) Financial Planning Division (DS/CFO/FP)

(CT:ORG-344; 08-29-2014)

The Financial Planning Division (DS/CFO/FP):

- (1) Safeguards all funds from misappropriation, waste, loss, and unauthorized use in compliance with all applicable laws and regulations;
- (2) Plans, develops, presents, justifies, and defends all DS funding requests to the Department, OMB and Congress;
- (3) Coordinates closely with DS/MGT/PPD to integrate the Bureau of Diplomatic Security's planning, budgeting, and performance evaluation process;
- (4) Serves as the primary liaison between DS and BP, the Office of Federal Assistance Financial Management (CGFS/FPRA/FAFM), and International Cooperative Administrative Support Services (CGFS/ICASS), about budget formulation matters;
- (5) Develops long-range and integrated financial planning strategies across appropriations that reflect interagency and Department coordination within the context of DS' overall planning and budgeting functions;
- (6) Provides financial estimates as part of the Bureau Strategic Resource Plan (BSRP) process by program performance goals and objectives, object class, program and organization;
- (7) Prepares documents for inclusion into briefing packages (e.g., questions and answers (Q&As) on budget issues, funding matrixes, history of funding requests and approvals, etc.) for the participation of DS senior officials in the critical events (e.g., annual bureau performance plan senior review, Congressional testimony, etc.);
- (8) Analyzes and evaluates the impact of authorization and appropriation legislation on DS resources and allocations;
- (9) Organizes and develops the annual financial plan and analyzes financial plan requests DS offices submit; DS/CFO/FP defends requests DS submitted to the Department for additional funding;
- (10) Monitors the execution of approved financial plan and recommends the reprogramming of resources to DS' senior management. DS/CFO/FP submits and defends unfunded requirements to BP during the quarterly review process;
- (11) Conducts monthly DS senior management meetings compiling unfunded requests throughout DS, creating briefing folders for senior managers with agenda and relevant materials for the meeting;

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

- (12) Allocates DS resources consistent with Department and DS policies, objectives, and applicable laws and regulations;
- (13) Ensures efficient and effective use of DS resources and analyzes and evaluates their use in accomplishing DS program objectives;
- (14) Analyzes funding requirements and expenditure trends in relation to Bureau and office functions;
- (15) Seeks ways to improve the overall financial management of DS resources, to ensure optimal resource management and use through special studies on resource issues addressing strategic planning, resource utilization, and operating requirements;
- (16) Coordinates the Bureau's ICASS initial and mid-year budget submissions for the DS Local Guard Program worldwide, identifying and justifying additional funding requirements for each;
- (17) Participates in and defends DS's ICASS budget for the Local Guard Program in ICASS working group meetings and hearings;
- (18) Performs management analyses of ICASS cost data on a macro and post level to derive more efficient and cost-effective management and delivery of local guard services; and
- (19) Reviews foreign exchange rate allotment adjustments for accuracy and analyzes and estimates the impact of foreign currency fluctuations on DS operations abroad.

1 FAM 263.3 Office of the Chief Technology Officer (DS/EX/CTO)

(CT:ORG-344; 08-29-2014)

The Office of the Chief Technology Officer (DS/EX/CTO) provides consolidated automated systems support for DS, including:

- (1) Data center operation, service desk, configuration management, and information security;
- (2) Software development, maintenance, installation, integration, training, and support;
- (3) Data communication, system networking, and video teleconferencing services or solutions; and
- (4) Capital planning, systems integration, project management, enterprise architecture and system planning, and business analysis and requirements.

1 FAM 263.3(A) Capital Planning and Architecture Division (DS/CTO/CPA)

(CT:ORG-344; 08-29-2014)

The Capital Planning and Architecture Division (DS/CTO/CPA) plans and aligns information technology (IT) investments strategically to Federal requirements, the Department mission, and DS' goals. This division ensures that DS priority investments are planned, funded, and managed adequately to accomplish their intended purpose. It is comprised of the following five functional areas:

- (1) Capital planning—provides results-oriented information on all matters related to the planning, budgeting, management, and control of IT capital investments, including the ongoing evaluation of the existing investment portfolio, and ensuring DS compliance with e-Governance reporting guidelines;
- (2) Systems integration—designs, evaluates, integrates, and implements IT systems solutions for DS;
- (3) Project management—responsible for evaluating, planning, organizing, and directing all IT projects for DS and ensuring that e-Governance principles are applied to all IT investments;
- (4) Enterprise architecture and systems planning—develops, maintains, and facilitates the implementation of an integrated IT architecture that aligns technology with business needs, Department enterprise architecture, and Federal enterprise architecture standards; and
- (5) Business analysis and requirements—reviews current business processes that impact IT projects and elicits, documents, and validates requirements of DS IT project stakeholders.

1 FAM 263.3(B) Systems Management Division (DS/CTO/SMD)

(CT:ORG-344; 08-29-2014)

The Systems Management Division (DS/CTO/SMD) manages software development and maintenance, information security, and overall information technology (IT) operations for the Bureau of Diplomatic Security (DS), including the DS Data Center, network management and service desk, and designs, develops, and deploys current, advanced technology to meet the Bureau's needs. DS/CTO/SMD acts as the primary liaison with the Bureau of Information Resource Management (IRM) for implementation and support of "in-scope" desktop support. It contains the following three functional areas:

- (1) Operations—operates the 24x7x365 DS Data Center and data centers in other annexes, runs the CTO service desk, applications support, manages networks and servers, and installs and maintains IT equipment;
- (2) Security operations—ensures the confidentiality, integrity, and availability

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

of DS automated information systems (AIS) by assuring that all systems comply with 5 FAM and 12 FAM regulations and Department security configuration guidelines, and approves and audits all user accounts; and

- (3) Software—performs full life-cycle management of software design, development, implementation, and maintenance, including database administration and Web and client/server application management, and performs limited end-user application training.

1 FAM 263.4 Human Resources Management (DS/EX/HRM)

(CT:ORG-344; 08-29-2014)

Human Resources Management (DS/EX/HRM):

- (1) Advises and makes recommendations to DS senior management, and the Executive Director (DS/EX) and Deputy Executive Director concerning all aspects of the Bureau's human resource management policies and programs; develops programs and implements the Bureau's human resource management policies and procedures;
- (2) Provides a full range of human resource management services to DS, e.g., recruitment and staffing, classification, compensation, training and development, employee relations, performance management, and employee benefits and services;
- (3) Provides workforce analysis, organizational planning and position management services worldwide, to DS management on the domestic DS workforce, and the workforce abroad identified as special agents, security engineering officers, security technical specialists, and diplomatic couriers;
- (4) Administers programs for the recruitment and examination of candidates for security-related Foreign Service positions, personal services contractors, and law enforcement availability pay (LEAP);
- (5) Makes decisions concerning Civil Service staffing and classification and recommends action to the DS/EX regarding employee relations cases from entry level through the GS-15 level, through Delegation of Personnel Authority from the Director General of the Foreign Service and the Director of Human Resources;
- (6) Analyzes and evaluates the effectiveness of DS' Human Resource Management Program; and
- (7) Acts as consultant to both management and employees about any issue concerning human resource management, policies, programs, or procedures.

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 1
Organization and Functions

1 FAM 264 THROUGH 269 UNASSIGNED

UNCLASSIFIED (U)

1 FAM EXHIBIT 261.2 BUREAU OF DIPLOMATIC SECURITY (DS)

(CT:ORG-344; 08-29-2014)

